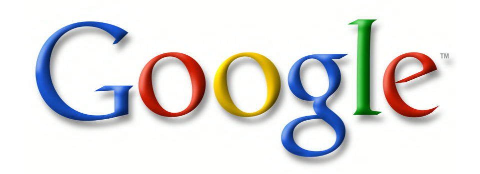



HARVARD
UNIVERSITY
LIBRARY

Das allgemeine quadratische Reciprocitätsgesetz

in

ausgewählten Kreiskörpern der $2^{h\text{ten}}$ Einheitswurzeln.

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der

hohen philosophischen Fakultät

der

Georg-Augusts-Universität zu Göttingen

vorgelegt von

Karl Sigismund Hilbert
aus Langenbielau in Schlesien.

Göttingen 1900.
Druck der Dieterich'schen Universitäts-Buchdruckerei
(W. Fr. Kaestner.)

Referent: Herr Prof. Dr. Hilbert.

Tag der mündlichen Prüfung: 18. Dezember 1899.

Einleitung.

In der Abhandlung von D. Hilbert „Ueber die Theorie des relativ quadratischen Zahlkörpers“ [1]) ist zum ersten Male das Reciprocitätsgesetz für quadratische Reste innerhalb eines algebraischen Grundkörpers k vollständig aufgestellt und bewiesen worden. Vorausgesetzt ist hierbei, dass der Grundkörper k nebst seinen sämmtlichen konjugirten Körpern imaginär ist und überdies eine ungerade Klassenanzahl besitzt.

Der nächste Zweck der vorliegenden Arbeit besteht darin, den Inhalt und die Richtigkeit des genannten Gesetzes, die durch einen sehr abstrakten Beweis verbürgt ist, an Zahlenbeispielen evident zu machen. Es wird dabei das Gesetz in der besonders leicht fasslichen und eleganten Darstellung zu Grunde gelegt werden, in welcher es der Entdecker desselben neuerdings in der Abhandlung „Ueber die Theorie der relativ Abel'schen Zahlkörper“ [2]) auf's Neue ausgesprochen hat.

Mögen ferner die Berechnungen der vorliegenden Arbeit noch als ein Versuch angesehen werden, zahlentheoretische Gesetze in Zahlkörpern höherer Grade als derjenigen zu bestätigen, von denen die gewöhnlich zu Beispielen verwendeten Grundkörper sind. Der Verfasser ist überdies von dem Bestreben geleitet worden, die zur Bestätigung erforderlichen Berechnungen möglichst allgemein zu halten und einem beliebig hohen Grade des gewählten Zahlkörpers anzupassen. Als Resultat dieses Bemühens sind die Sätze des § 4 hervorgegangen, nach denen die Bestimmung des quadratischen Charakters einer beliebigen Zahl des gewählten Zahlkörpers nach einem beliebigen Modul stets zurückgeführt

1) Mathematische Annalen Bd. 51.

2) Nachrichten d. K. Ges. d. Wiss. zu Göttingen 1898.

werden kann auf die Bestimmung des quadratischen Charakters rationaler Zahlen im Körper der rationalen Zahlen.

Bei dem Bestreben nach Allgemeinheit hinsichtlich des Grades war es wünschenswert, einen möglichst einfachen Zahlkörper zur Berechnung heranzuziehen. Die moderne Zahlentheorie lehrt, dass die absolute Grösse und die Anzahl der in der Körperdiskriminante aufgehenden rationalen Primzahlen ein Kriterium für die Einfachheit eines Zahlkörpers liefern. Darnach bieten sich zunächst die Kreiskörper mit Primzahl- bezw. Primzahlpotenz-Exponenten als die einfachsten dar; für diese besitzen wir überdies ein ausgezeichnetes Zahlenmaterial in den „Tafeln komplexer Primzahlen, welche aus Wurzeln der Einheit gebildet sind", einem Werk, welches auf Anregung von Kummer von Herrn Prof. C. G. Reuschle hergestellt ist. Die Einheitswurzeln, von welchen der Titel des Werkes spricht, sind die imaginären Wurzeln der Einheit, deren Grade die sämmtlichen Zahlen des ersten Hunderts sind.

Wir haben den Kreiskörper der $2^{h\text{ten}}$ Einheitswurzeln $k\left(e^{\frac{2i\pi}{2^h}}\right)$ gewählt, dessen Diskriminante eine Potenz der kleinsten rationalen Primzahl, der 2, ist. Obwohl dieser Zahlkörper von gewissen Eigenthümlichkeiten ist, die ihn gerade vor anderen Kreiskörper auszeichnen und vor mehreren Jahren von Heinrich Weber zum Gegenstande besonderer Untersuchungen gemacht worden sind, so erweist derselbe sich doch für die hier zum Ziele gesteckten Berechnungen, wie man sehen wird, als ganz besonders einfach und durchsichtig.

Die speciellen Körper, in welchen das allgemeine quadratische Reciprocitätsgesetz bestätigt werden wird, sind die Zahlkörper der vierten, achten und sechszehnten Einheitswurzeln. Den Bestätigungen lassen wir noch einen allgemeinen Teil voraufgehen. In den drei ersten Paragraphen wird eine vollständige zahlentheoretische Analysis des Zahlkörpers und seines Integritätsbereiches dargeboten; im vierten Paragraphen wird die bereits erwähnte Untersuchung über die quadratischen Charaktere durchgeführt.

---

§ 1.

Allgemeine Charakterisirung des Kreiskörpers der $2^{h\text{ten}}$ Einheitswurzeln.

Der Zahlkörper, welchen wir betrachten, entspringt aus einer primitiven Wurzel der Gleichung

$$F(x) = x^{2^h} - 1 = 0.$$

Die Gleichung der primitiven Wurzeln von $F(x) = 0$ ist

$$f(x) = x^{2^{h-1}} + 1 = 0;$$

dieselbe ist irreducibel im Bereich der rationalen Zahlen und besitzt nur imaginäre Wurzeln, von denen jede eine bestimmte Potenz von irgend einer unter denselben ist. $Z = e^{\frac{2i\pi}{2^h}}$ ist eine Wurzel der Gleichung $f(x) = 0$ und die sämmtlichen Wurzeln derselben sind

$$Z^1,\ Z^3,\ Z^5,\ \ldots\ldots,\ Z^{2^h-1}.$$

Die Exponenten von Z bilden die Reihe aller ungeraden Zahlen unterhalb 2^h. Nun haben die Zahlen 3 und 5, oder auch die Zahlen $2^h - 3$ und $2^h - 5$, und nur diese Zahlen die Eigenschaft, dass jede ungerade Zahl unterhalb 2^h, abgesehen vom Vorzeichen $+$ oder $-$, einer bestimmten Potenz von 3 bezw. 5 nach dem Modul

2^λ kongruent ist. Bezeichnet man mit $2n+1$ eine ungerade Zahl $\leqq 2^\lambda - 1$, so bestehen nach 2^λ die Kongruenzen

$$2n+1 \equiv (-1)^{\frac{n(n-1)}{2}} \cdot 3^e$$
$$2n+1 \equiv (-1)^n \cdot 5^{e'}.$$

Im Besonderen sei hierzu bemerkt, dass die $2^{\lambda-1}$ ungeraden Zahlen unterhalb 2^λ sich stets so in zwei gleichviel $2^{\lambda-2}$ Zahlen enthaltende Gruppen teilen lassen, dass die Zahlen der einen Gruppe kongruent $+3^e$ bezw. $+5^{e'}$ ausfallen, wo e, e' die Werte $1, 2, 3, \ldots 2^{\lambda-2}$ annehmen, und dass die Zahlen der anderen Gruppe kongruent -3^e bezw. $-5^{e'}$ ausfallen, wo wieder e, e' gleich $1, 2, 3, \ldots 2^{\lambda-2}$ werden. Hieraus folgt, dass $2^{\lambda-2}$ der niedrigste Exponent ist, für welchen 3^e bezw. $5^{e'}$ kongruent 1 nach 2^λ ausfallen; denn wäre

$$3^\varkappa \equiv 5^{\varkappa'} \equiv 1, \quad (2^\lambda),$$

wo $\varkappa, \varkappa'$ kleiner als $2^{\lambda-2}$, so wäre

$$3^{\varkappa+1} \equiv 3^1, \quad 5^{\varkappa'+1} \equiv 5^1, \quad (2^\lambda)$$

und daher wären die Potenzen 3^e bezw. $5^{e'}$ für $e'\, e$ gleich $1, 2, 3, \ldots 2^{\lambda-2}$ nicht sämmtlich von einander verschieden.

Hieraus folgt, dass die Gruppe des Körpers $K(Z)$, wenn man $s = (Z : Z^5)$, $t = (Z : Z^3)$, $s' = (Z : Z^{-1})$ setzt, folgende beiden Darstellungen gestattet:

$$s = (Z : Z^5), \quad s^2 = \left(Z : Z^{5^2}\right), \quad \ldots, \quad s^{2^{\lambda-2}} = \left(Z : Z^{5^{2^{\lambda-2}}}\right) = 1,$$
$$s's = (Z : Z^{-5}), \quad s's^2 = \left(Z : Z^{-5^2}\right), \quad \ldots, \quad s^{2^{\lambda-2}}s' = \left(Z : Z^{-5^{2^{\lambda-2}}}\right) = s',$$

und ferner:

$$t = (Z : Z^3), \quad t^2 = \left(Z : Z^{3^2}\right), \quad \ldots, \quad t^{2^{\lambda-2}}\left(Z : Z^{3^{2^{\lambda-2}}}\right) = 1,$$
$$s't = (Z : Z^{-3}), \quad s't^2 = \left(Z : Z^{-3^2}\right), \quad \ldots, \quad s't^{2^{\lambda-2}} = \left(Z : Z^{3^{2^{\lambda-2}}}\right) = s'.$$

Die Substitutionen der Gruppe des Körpers $K(Z)$ setzen sich zusammen aus den Potenzen von s, bezw. t, und den Produkten dieser Potenzen mit s'.

Diese Darstellungen der Gruppe des Körpers $K(Z)$, dessen Grad wir jetzt mit m bezeichnen, indem wir $2^{\lambda-1} = m$ setzen,

besagen, dass der Körper $K(Z)$ sich zusammensetzen lässt aus dem reellen Körper $k(Z+Z^{-1})$ vom Grade $\frac{m}{2}$ und einem der beiden imaginären quadratischen Körper $k(i)$ oder $k(\sqrt{-2})$.

Beweis. Die Substitution $s = (Z:Z^5)$ also auch deren Potenzen, lassen die Zahl $Z^{\frac{m}{2}} = i$, die Substitution $t = (Z:Z^3)$ und deren Potenzen lassen die Zahl $Z^{\frac{m}{4}} - Z^{-\frac{m}{4}} = \sqrt{i} - \sqrt{i}^{-1} = \sqrt{-2}$, die Substitution $s' = (Z:Z^{-1})$, $s'^2 = 1$ lassen die reelle Zahl

$$Z + Z^{-1} = e^{\frac{2i\pi}{2^h}} = e^{-\frac{2i\pi}{2^h}} = 2\cos\frac{2\pi}{2^h}$$

umgeändert.

Der reelle Körper $k(Z+Z^{-1})$ ist cyklisch, seine Substitutionsgruppe darstellbar durch die Potenzen

$$s,\ s^2,\ \ldots,\ s^{\frac{m}{2}},$$

oder durch die Potenzen

$$t,\ t^2,\ \ldots,\ t^{\frac{m}{2}}.$$

Die zu $k(Z+Z^{-1})$ gehörige Untergruppe vom Grade 2 ist

$$\sigma = (Z:Z^{-1}), \quad \sigma^2 = 1.$$

Neben den reellen cyklischen Unterkörper $k(Z+Z^{-1})$ vom Grade $\frac{m}{2}$ stellt sich ein imaginärer cyklischer Unterkörper vom gleichen Grade. Dieser Unterkörper wird bestimmt durch die imaginäre Zahl

$$Z - Z^{-1} = e^{\frac{2i\pi}{2^h}} - e^{-\frac{2i\pi}{2^h}} = 2i\sin\frac{2\pi}{2^h}.$$

Die Substitutionsgruppe dieses Körpers $k(Z-Z^{-1})$ ist durch dieselben Substitutionen darstellbar, wie diejenige des Körpers $k(Z+Z^{-1})$. Die zu $k(Z-Z^{-1})$ gehörende Untergruppe zweiten Grades ist

$$\sigma = (Z : -Z^{-1}), \quad \sigma^2 = 1.$$

Der dritte noch existirende Unterkörper vom Grade $\frac{m}{2}$ ist nicht cyklisch und von demselben Typus wie $K(Z)$; derselbe wird definirt durch die Zahl Z^2 und die Gleichung $(Z^2)^{\frac{m}{2}} + 1 = 0$.

Genau so wie sich vom Körper $K(Z)$ vom Grade m drei Unterkörper vom Grade $\frac{m}{2}$ ableiten, so leiten sich vom Körper $k(Z^2)$ vom Grade $\frac{m}{2}$ drei Unterkörper vom Grade $\frac{m}{4}$ ab. Es sind dies erstens der Körper $k(Z^4)$, der nicht cyklisch und von demselben Typus wie $K(Z)$ ist, zweitens der reelle cyklische Körper $k(Z^2+Z^{-2})$ und drittens der imaginäre cyklische Körper $k(Z^2-Z^{-2})$.

Zur Uebersicht schreiben wir jetzt die sämmtlichen Unterkörper des Körpers $K(Z) = K\left(e^{\frac{2i\pi}{2^\lambda}}\right)$ in drei Reihen, nach absteigenden Graden ordnend.

I. Die nichtcyklischen imaginären Unterkörper.

$$\left.\begin{array}{lll}
k\left(e^{\frac{2i\pi}{2^{\lambda-1}}}\right) = k(Z^2): & \text{Gleichung} & x^{\frac{m}{2}}+1 = 0, \\
k\left(e^{\frac{2i\pi}{2^{\lambda-2}}}\right) = k(Z^4): & \text{„} & x^{\frac{m}{4}}+1 = 0, \\
k\left(e^{\frac{2i\pi}{2^{\lambda-3}}}\right) = k(Z^8): & \text{„} & x^{\frac{m}{8}}+1 = 0, \\
\cdots\cdots & \cdots\cdots & \cdots\cdots \\
k\left(e^{\frac{2i\pi}{2^5}}\right) = k(\sqrt[8]{i}): & \text{„} & x^{16}+1 = 0, \\
k\left(e^{\frac{2i\pi}{2^4}}\right) = k(\sqrt[4]{i}): & \text{„} & x^{8}+1 = 0, \\
k\left(e^{\frac{2i\pi}{2^3}}\right) = k(\sqrt{i}): & \text{„} & x^{4}+1 = 0, \\
k\left(e^{\frac{2i\pi}{2^2}}\right) = k(i): & \text{„} & x^{2}+1 = 0, \\
k\left(e^{\frac{2i\pi}{2}}\right) = k(-1): & \text{„} & x+1 = 0,
\end{array}\right\} \text{I.}$$

II. Die cyklischen imaginären Unterkörper.

$k(Z-Z^{-1})$:	Grad: $\frac{m}{2}$,	II.
$k(Z^2-Z^{-2})$:	„ $\frac{m}{4}$,	
$k(Z^4-Z^{-4})$:	„ $\frac{m}{8}$,	
$k(Z^8-Z^{-8})$:	„ $\frac{m}{16}$,	
. . . .	. . .	
$k\left(\sqrt{-2+\sqrt{-2+\sqrt{-2+\sqrt{2}}}}\right)$:	Grad: 16,	
$k\left(\sqrt{-2+\sqrt{-2+\sqrt{2}}}\right)$:	„ 8,	
$k\left(\sqrt{-2+\sqrt{2}}\right)$:	„ 4,	
$k(\sqrt{-2})$:	„ 2,	
$k(0)$:	„ 0.	

III. Die cyklischen reellen Unterkörper.

$k(Z+Z^{-1})$:	Grad: $\frac{m}{2}$,	III.
$k(Z^2+Z^{-2})$:	„ $\frac{m}{4}$,	
$k(Z^4+Z^{-4})$:	„ $\frac{m}{8}$,	
$k(Z^8+Z^{-8})$:	„ $\frac{m}{16}$,	
. . . .	. . .	
$k\left(\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}\right)$:	„ 16,	
$k\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$:	„ 8,	
$k\left(\sqrt{2+\sqrt{2}}\right)$	„ 4,	
$k(\sqrt{2})$:	„ 2,	
$k(0)$:	„ 0.	

Jeder nichtcyklische imaginäre Körper der Reihe I, abgesehen von $k(\sqrt{-1})$, enthält von einem bestimmten Grade, $2^{\varkappa}$, $2 \leqq \varkappa \leqq h-2$, stets drei und nur drei Unterkörper, einen nichtcyklischen imaginären der Reihe I, einen cyklischen imaginären der Reihe II, einen cyklischen reellen der Reihe III.

Zweitens beweisen wir folgenden Satz:

Die beiden cyklischen Unterkörper, der imaginäre $k(Z-Z^{-1})$ und der reelle $k(Z+Z^{-1})$ enthalten von einem bestimmten Grade, $2^{\varkappa}$, $1 \leqq \varkappa \leqq h-2$, stets einen und nur einen Unterkörper. Derselbe ist ein reeller cyklischer der Reihe III.

Beweis. Jede Zahl α des Körpers $k(Z+Z^{-1})$ ist, da $\frac{m}{2}$ der Grad desselben, in folgender Form darstellbar:

$$\begin{aligned}\alpha = a_0 + a_1(Z+Z^{-1}) + a_2(Z+Z^{-1})^2 \\ + a_3(Z+Z^{-1})^3 + a_4(Z+Z^{-1})^4 \\ + \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ + a_{\frac{m}{2}-1} \cdot (Z+Z^{-1})^{\frac{m}{2}-1},\end{aligned}$$

wo a_0, a_1, a_2, ... rationale Zahlen bezeichnen. Dieser Ausdruck für α lässt sich leicht auf den folgenden reduciren:

$$\begin{aligned}\alpha = r_0 + r_1(Z+Z^{-1}) + r_2(Z^2+Z^{-2}) \\ + r_3(Z^3+Z^{-3}) + r_4(Z^4+Z^{-4}) \\ + \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ + r_{\frac{m}{2}-1}\left(Z^{\frac{m}{2}-1} + Z^{-\frac{m}{2}+1}\right),\end{aligned}$$

wo wieder r_0, r_1, r_2, ... rationale Zahlen bezeichnen. Es ist nun sofort ersichtlich, dass die in Klammer stehenden Binome nur Zahlen von Körpern $k(Z^{2^{\varkappa}} + Z^{-2^{\varkappa}})$, d. h. Zahlen von Körpern der Reihe III darstellen. In der That sind die Binome nur von einer der folgenden drei Formen

$$Z^{2n+1}+Z^{-(2n+1)}$$

$$Z^{2^\lambda.(2n+1)}+Z^{-2^\lambda.2n+1)}$$

$$Z^{2^\varkappa}+Z^{-2^\varkappa}.$$

Die Zahl $Z^{2n+1}+Z^{-(2n+1)}$ ist entweder identisch mit der Zahl $Z+Z^{-1}$ oder zu dieser letzteren konjugirt im Körper $k(Z+Z^{-1})$; denn die erstere entsteht aus der letzteren durch eine Substitution $\sigma = (Z:Z^{2n+1})$, d. h. durch eine Substitution der Gruppe von $K(Z)$, durch welche die Zahlen des Körpers $k(Z+Z^{-1})$ entweder ungeändert gelassen oder in ihre konjugirten übergeführt werden. Desgleichen ist die Zahl $Z^{2^\lambda.(2n+1)}+Z^{-2^\lambda.2n+1)}$ eine Zahl des Körpers $k(Z^{2^\lambda}+Z^{-2^\lambda})$, durch die Substitution $\sigma = (Z:Z^{2n+1})$ aus der Zahl $Z^{2^\lambda}+Z^{-2^\lambda}$ hervorgegangen. Wie man also auch über die Koëfficienten r_0, r_1, r_2, ... verfügen mag, man kann für α nur Zahlen erhalten, welche einem der Körper der Reihe III angehören, womit die Behauptung, soweit sie den Körper $k(Z+Z^{-1})$ angeht, bewiesen ist.

Aus dem binomischen Satze folgt ferner, dass eine beliebige Zahl α des Körpers $k(Z-Z^{-1})$ sich in folgender Form darstellen lässt

$$\begin{aligned}\alpha = &\sum a\cdot\left(Z^{2n+1}-Z^{-(2n+1)}\right)\\ &+\sum b\cdot\left(Z^{2^\lambda(2n+1)}+Z^{2^\lambda.(2n+1)}\right)\\ &+\sum c\cdot\left(Z^{2^\varkappa}+Z^{-2^\varkappa}\right),\end{aligned}$$

wo a, b, c rationale Zahlenkoefficienten bezeichnen. Da nun $Z^{2n+1}-Z^{-(2n+1)}$ entweder identisch mit $Z-Z^{-1}$ oder zu dieser Zahl konjugirt, so folgt, dass die Unterkörper von $k(Z-Z^{-1})$ vollkommen identisch sind mit denjenigen des Körpers $k(Z+Z^{-1})$. Hiermit ist der obige Satz vollständig bewiesen.

Wir verlassen jetzt die Diskussion des Körpers $K(Z)$ im Allgemeinen und suchen den Bereich der ganzen Zahlen desselben, den Integritätsbereich nach Kronecker's Ausdrucksweise, insbesondere die Primideale und Einheiten zu erforschen.

§ 2.

Die Zerlegung der Zahl 2, die Diskriminante, die ganzen Zahlen des Zahlkörpers $K\left(e^{\frac{2i\pi}{2}}\right)$.

Die Zahl 2 nimmt im Körper der $2^{h\text{ten}}$ Einheitswurzeln eine besondere Stellung ein, was darin seinen Grund hat, dass die Diskriminante dieses Körpers, wie weiterhin gezeigt werden wird, gleich einer gewissen Potenz von 2 ist.

Es gilt nämlich der Satz, dass die Diskriminante eines algebraischen Zahlkörpers alle und nur diejenigen rationalen Primzahlen als Faktoren enthält, welche durch das Quadrat eines Primideals teilbar sind.

Die Primfaktoren der Zahl 2 im Körper $K\left(e^{\frac{2i\pi}{2^h}}\right) = K(Z)$ lassen sich sehr leicht bestimmen. Da $Z^1, Z^3, Z^5, \ldots Z^{2m-1}$ die Wurzeln von $f(x) = x^m + 1 = 0$ sind, so gilt identisch in x:

$$f(x) = x^m + 1 = (x - Z^1)(x - Z^3)(x - Z^5) \ldots (x - Z^{2m-1});$$

setzt man $x = 1$, so kommt:

$$f(1) = 2 = (1 - Z^1)(1 - Z^5)(1 - Z\;) \ldots (1 - Z^{2m-1}).$$

Die Faktoren dieses Produktes unterscheiden sich von dem ersten Faktor $1 - Z$ nur um einen Einheitsfaktor. Es ist $\frac{1 - Z^g}{1 - Z}$, so oft g eine ungerade Zahl, eine Einheit von $K(Z)$; denn, ist g' eine ganze rationale Zahl von der Art, dass $g \cdot g' \equiv 1, (2m)$ ausfällt, so sind

$$E_g = \frac{1 - Z^g}{1 - Z}$$

sowie der reciproke Wert davon

$$E_g^{-1} = \frac{1 - Z}{1 - Z^g} = \frac{1 - Z^{gg'}}{1 - Z^g}$$

ganze Zahlen des Körpers $K(Z)$; es ist

$$\frac{1-Z^{\varrho}}{1-Z} = 1+Z+Z^2+\cdots+Z^{\varrho-1},$$

$$\frac{1-Z}{1-Z^{\varrho}} = \frac{1-Z^{\varrho\varrho'}}{1-Z^{\varrho}} = 1+Z^{\varrho}+Z^{2\varrho}+\cdots+Z^{(\varrho'-1)\varrho}.$$

Schreibt man jetzt obige Produktentwicklung der Zahl 2 in der Form

$$2 = (1-Z)\cdot\left(\frac{1-Z^3}{1-Z}\right)(1-Z)\cdot\left(\frac{1-Z^5}{1-Z}\right)\cdot(1-Z)\ldots$$

$$\ldots\ldots\ (1-Z)\left(\frac{1-Z^{2m-1}}{1-Z}\right),$$

so ersieht man daraus, dass

$$2 = (1-Z)^m$$

ist, sofern wir $(1-Z)$ als Hauptprimideal auffassen. Bezeichnen wir mit λ die Zahl $1-Z$ und mit $\mathfrak{l}$ das Hauptideal (λ), so erhalten wir die Gleichung

$$2 = \lambda^m\cdot E_3\cdot E_5\cdots E_{2m-1} = \mathfrak{l}^m.$$

Um die Diskriminante des Körpers $K(Z)$ zu bestimmen, nehmen wir den Ausgangspunkt von der Bestimmung der Differente δ der Zahl Z in $K(Z)$. Es ist

$$\delta = (Z-Z^3)(Z-Z^5)\cdots(Z-Z^{2m-1}) = \left[\frac{df(x)}{dx}\right]_{x=Z}.$$

Aus $(x^m-1)\cdot f(x) = x^{2m}-1$ folgt

$$(x^m-1)\frac{df(x)}{dx}+mx^{m-1}\cdot f(x) = 2mx^{2m-1}$$

und hieraus folgt:

$$(Z^m-1)\,\delta+m\,Z^{m-1}\cdot f(Z) = 2m\,Z^{2m-1},$$

d. h., da $f(Z) = 0$ und $Z^m-1 = 2$,

$$\delta = m\cdot Z^{2m-1}.$$

Jetzt benutzen wir den Satz, dass die Diskriminante einer Zahl bis auf das Vorzeichen gleich der Norm der Differente ist und dass das Vorzeichen gleich $(-1)^{\frac{m(m-1)}{2}}$, wenn m der Grad

des Körpers ist. Da in unserem Falle $m = 2^{h-1}$ ist, so wird $(-1)^{\frac{m(m-1)}{2}}$ ausser dem einzigen Falle $h = 2$, stets gleich $+1$. Es ist also die Diskriminante der Zahl Z

$$d(Z) = n(\delta),$$

d. h., da Z^{2m-1} eine Wurzel von $f(x) = 0 = x^m + 1 = 0$, also $n(Z^{2m-1}) = +1$, und da $n(m) = m^m$,

$$d(Z) = m^m = +2^{2^{h-1}(h-1)}.$$

Im Falle $m = 2$, $h = 2$, ist

$$d(Z) = d(i) = -2^2.$$

Nun ist aber die Diskriminante der Zahl Z gleich der Diskriminante des Körpers $K(Z)$, was daraus folgt, dass die Potenzen von Z:

$$Z^0,\ Z^1,\ Z^2,\ Z^3,\ \ldots\ Z^{m-1}$$

eine Basis des Körpers $K(Z)$ darstellen. Wir zeigen dies, indem wir folgenden Satz beweisen:

Jede ganze Zahl α des Körpers $K(Z)$ gestattet folgende Darstellung:

$$\alpha = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_{m-1} Z^{m-1},$$

wo $a_0,\ a_1,\ a_2 \ldots a_{m-1}$ ganze rationale Zahlen bezeichnen.

Beweis. Nach einem Elementarsatze der Theorie des algebraischen Zahlkörpers gestattet jede ganze Zahl ω des Körpers $K(Z)$, wenn α eine bestimmende Zahl desselben ist, die Darstellung

$$\omega = \frac{A_0 + A_1\alpha + A_2\alpha^2 + \cdots + A_{m-1}\alpha^{m-1}}{d(\alpha)},$$

wo $A_0,\ A_1,\ \ldots,\ A_{m-1}$ ganze rationale Zahlen und $d(\alpha)$ die Diskriminante von α bezeichnen. Wählen wir $\lambda = 1 - Z$ als bestimmende Zahl von $K(Z)$, so erhalten wir für ω die Darstellung

$$\omega = \frac{A_0 + A_1\lambda + A_2\lambda^2 + \cdots + A_{m-1}\lambda^{m-1}}{d(\lambda)},$$

oder, da die Diskriminante von λ gleich derjenigen von Z ist, weil die Differenten dieser Zahlen offenbar übereinstimmen,

$$\omega = \frac{A_0 + A_1\lambda + A_2\lambda^2 + \cdots + A_{m-1}\lambda^{m-1}}{2^{2^{h-1}(h-1)}};$$

hier sind die Koefficienten $A_0, A_1, \ldots$ sämmtlich durch $2^{2^{h-1}\cdot h-1}$ teilbar; denn zunächst ist, $2^{2^{h-1}}\cdot h - 1 = \varkappa$ gesetzt,

$$\omega\cdot 2^{\varkappa} = A_0 + A_1\lambda + \cdots + A_{m-1}\lambda^{m-1} \equiv 0,\ (2^{\varkappa}),$$

folglich, da $\quad 2 = \mathfrak{l}^m,\ \mathfrak{l} = (\lambda),$

$$A_0 \equiv 0,\ (\lambda),$$

also auch $\quad A_0 \equiv 0,\ (2).$

Daher wieder muss $\quad A_1\lambda \equiv 0,\ (\lambda^2)$

d. h. $\quad A_1 \equiv 0,\ (2)$ sein u. s. f.

Nachdem man so gezeigt hat, dass die Koefficienten $A_0, A_1, \ldots$ ein erstes Mal durch 2 teilbar sein müssen, zeigt man durch geeignete Weiterführung des eben angewandten Verfahrens, dass $A_0, A_1, \ldots$ sämmtlich durch $2^{2^{h-1}(h-1)}$ teilbar sind, dass also ω dargestellt wird durch

$$\omega = B_0 + B_1\lambda + B_2\lambda^2 + \cdots + B_{m-1}\lambda^{m-1},$$

wo $B_0, B_1, \ldots B_{m-1}$ ganze rationale Zahlen sind; hieraus folgt, da $\lambda = 1 - Z$,

$$\omega = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_{m-1} Z^{m-1},$$

wie oben behauptet wurde.

§ 3.

Die Zerlegung der ungeraden rationalen Primzahlen in Primideale des Kreiskörpers der $2^{h\text{ten}}$ Einheitswurzeln.

Es werde mit $k^{(e)}$ irgend ein in $K(Z)$ enthaltener Unterkörper vom Grade e mit der ihm zugehörenden Untergruppe U_f, vom Grade $f = \frac{m}{e}$, oder auch der Körper $K(Z)$ selbst bezeichnet, in welchem Falle $e = m$ ist und die Untergruppe sich auf die identische Substitution $\sigma = (Z:Z) = 1$ reducirt. Wir beweisen dann folgenden **Satz 1**:

Ist $\mathfrak{p}$ ein in der ungeraden rationalen Primzahl p aufgehendes Primideal ersten Grades des Körpers $k_{\mathfrak{i}}^{(e)}$, so ist die Substitution

$$\sigma = (Z : Z^p)$$

eine Substitution der zu $k^{(e)}$ gehörenden Untergruppe U_f.

Ist dann f' der kleinste positive Exponent von p, für welchen

$$p^{f'} \equiv 1, \quad (2^h)$$

ausfällt, so sind die Substitutionen

$$\sigma = \left(Z : Z^p\right), \quad \sigma^2 = \left(Z : Z^{p^2}\right), \quad \ldots, \quad \sigma^{f'} = \left(Z : Z^{p^{f'}}\right)$$

sämmtlich von einander verschiedene Substitutionen der Untergruppe U_f.

Beweis. Der Körper $K(Z)$ besitzt, wie gezeigt worden, von einem Grade e drei Unterkörper, deren bestimmende Zahlen folgende sind

$$Z^{\frac{m}{e}}, \quad Z^{\frac{m}{2e}} + Z^{-\frac{m}{2e}}, \quad Z^{\frac{m}{2e}} - Z^{-\frac{m}{2e}}.$$

Sei zuerst $k^{(e)}$ identisch mit $k\left(Z^{\frac{m}{e}}\right)$, so ist nach dem Fermat'schen Satze

$$Z^{\frac{m}{e}(p-1)} \equiv 1, \quad (\mathfrak{p})$$

oder

$$Z^{\frac{m}{e}(p-1)} - 1 \equiv 0, \quad (\mathfrak{p}).$$

Nun geht aber die Zahl

$$Z^{\frac{m}{e}(p-1)} - 1$$

in der Zahl 2 auf, ausgenommen den Fall, dass

$$\frac{m}{e}(p-1) \equiv 0, \quad (2m),$$

also identisch

$$Z^{\frac{m}{e}(p-1)} - 1 = 0$$

oder

$$Z^{\frac{m}{e}p} = Z^{\frac{m}{e}}$$

ist. Da nun $\mathfrak{p}$ n. V. prim zu 2 ist, so muss die letzte Identität stattfinden, d. h. es muss die Substitution

$$\sigma = (Z : Z^p)$$

eine Substitution der zu $k^{(e)} = k\left(Z^{\frac{m}{e}}\right)$ gehörenden Untergruppe sein.

Ist ferner $k^{(e)}$ identisch mit $k\left(Z^{\frac{m}{2e}} + Z^{-\frac{m}{2e}}\right)$, so ist wieder nach dem Fermat'schen Satze:

$$\left(Z^{\frac{m}{2e}} + Z^{-\frac{m}{2e}}\right)^p \equiv Z^{\frac{m}{2e}} + Z^{-\frac{m}{2e}}, \quad (\mathfrak{p});$$

da nun nach einem bekannten Satze aus der Theorie der Kongruenzen

$$\left(Z^{\frac{m}{2e}} + Z^{-\frac{m}{2e}}\right)^p \equiv Z^{p\frac{m}{2e}} + Z^{-p\frac{m}{2e}}$$

nach $(\mathfrak{p})$ und also erst recht nach (p), so ist infolge der ersten Kongruenz

$$Z^{p\frac{m}{2e}} + Z^{-p\frac{m}{2e}} \equiv Z^{\frac{m}{2e}} + Z^{-p\frac{m}{2e}}, \quad (\mathfrak{p}).$$

Dieser letzten Kongruenz erteilen wir eine andere Gestalt. Zunächst ist

$$Z^{p\frac{m}{2e}} - Z^{-\frac{m}{2e}} + Z^{-p\frac{m}{2e}} - Z^{\frac{m}{2e}} \equiv 0, \quad (\mathfrak{p}).$$

Die linke Seite dieser Kongruenz schreiben wir folgendermassen als Produkt

$$Z^{\frac{m}{2e}}\left(1 - Z^{-\frac{m}{2e}(p+1)}\right)\left(1 - Z^{\frac{m}{2e}(p-1)}\right) \equiv 0, \quad (\mathfrak{p})$$

oder, indem wir die Kongruenz mit der Einheit $-Z^{\frac{m}{2e}p}$ multipliciren

$$\left(1 - Z^{\frac{m}{2e}(p+1)}\right)\left(1 - Z^{\frac{m}{2e}(p-1)}\right) \equiv 0, \quad (\mathfrak{p}).$$

Einer der beiden Faktoren muss gleich Null sein, da sonst beide Faktoren Teiler von 2 sind, und mithin ist

$$-Z^{p\frac{m}{2e}} - Z^{-p\frac{m}{2e}} + Z^{\frac{m}{2e}} + Z^{-\frac{m}{2e}} = 0,$$

oder

$$Z^{p\frac{m}{2e}} + Z^{-p\frac{m}{2e}} = Z^{\frac{m}{2e}} + Z^{-\frac{m}{2e}},$$

d. h. $\sigma = (Z : Z^p)$ ist eine Substitution der zu $k\left(Z^{\frac{m}{2e}} + Z^{-\frac{m}{2e}}\right)$ gehörenden Untergruppe.

In ganz entsprechender Weise wird bewiesen, dass, wenn $k^{(e)} = k\left(Z^{\frac{m}{2e}} - Z^{-\frac{m}{2e}}\right)$ ist, die Substitution $\sigma = (Z : Z^p)$ der zu $k^{(e)}$ gehörenden Untergruppe angehört.

Hiermit ist der erste Teil obigen Satzes bewiesen.

Sei jetzt f' der kleinste positive Exponent von p, für welchen

$$p^{f'} \equiv 1, \quad (2^{\lambda})$$

ausfällt, so werden die Substitutionen

$$\sigma = (Z : Z^p), \quad \sigma^2 = (Z : Z^{p^2}), \quad \dots, \quad \sigma^{f'} = (Z : Z^{p^{f'}})$$

sämmtlich die bestimmende Zahl von $k^{(e)}$ ungeändert lassen und also der Untergruppe U_f angehören. Ferner aber sind die Substitutionen $\sigma, \sigma^2, \dots, \sigma^{f'}$ sämmtlich von einander verschiedene Substitutionen der Gruppe von $K(Z)$, da die Potenzen $p, p^2, \dots, p^{f'}$ sämmtlich einander inkongruent nach 2^{λ} sind. In der That, wäre etwa

$$p^{f_1} \equiv p^{f_2}, \quad (2^{\lambda}),$$

wo $f_1 < f'$ und $f_2 \neq f_1$, etwa $f_2 > f_1$, und $f_2 \leqq f'$, so würde aus

$$p^{f_1} \equiv p^{f_2}, \quad (2^{\lambda})$$

folgen

$$p^{f_1}(1 - p^{f_2 - f_1}) \equiv 0, \quad (2^{\lambda}).$$

Da nun

$$p^{f_1} \not\equiv 0, \quad (2),$$

so müsste

$$p^{f_2 - f_1} \equiv 1, \quad (2^{\lambda})$$

sein, was der Voraussetzung widerspricht.

Da also $\sigma, \sigma^2, \ldots, \sigma^{f'}$ sämmtlich verschiedene Substitutionen der Gruppe von $K(Z)$ sind und sämmtlich der Untergruppe U_f angehören, so sind sie auch sämmtlich verschiedene Substitutionen der Untergruppe U_f.

Damit ist die Behauptung vollständig bewiesen. Wir ziehen aus derselben die Folgerung

$$f' \leqq f.$$

Da nun ein Primideal des Körpers $K(Z)$ entweder vom ersten Grade in $K(Z)$ oder vom ersten Grade in einem Unterkörper $k^{(e)}$ sein muss, so dürfen wir annehmen, $\mathfrak{p}$ sei ein Primideal von $K(Z)$, und wir beweisen dann den **Satz 2**:

Ist $\mathfrak{p}$ ein in der ungeraden rationalen Primzahl p aufgehendes Primideal des Körpers $K(Z)$, welches vom ersten Grade im Unterkörper $k^{(e)}$, so ist

$$f = \frac{m}{e}$$

der niedrigste Exponent von p, für welchen $p^f \equiv 1, \ (2^\lambda)$ wird. Die Zerlegung von p in $K(Z)$ ist

$$p = \mathfrak{p}_1 \ldots\ldots \mathfrak{p}_e,$$

wo $\mathfrak{p}_1 \ldots\ldots \mathfrak{p}_e$ von einander verschiedene Primideale ersten Grades in $k^{(e)}$ sind.

Beweis. Sei f' der niedrigste Exponent von p, für welchen $p^{f'} \equiv 1, \ (2^\lambda)$ ausfällt, so gilt, wenn $f(Z)$ eine beliebige ganze Zahl von $K(Z)$ ist, die Kongruenz

$$f(Z)^{p^{f'}} \equiv f(Z^{p^{f'}}) \equiv f(Z), \quad (p),$$

also ist um so mehr

$$f(Z)^{p^{f'}} \equiv f(Z), \quad (\mathfrak{p}),$$

d. h. die Kongruenz

$$\mathfrak{x}^{p^{f'}} - \mathfrak{x} \equiv 0, \quad (\mathfrak{p})$$

wird von jeder ganzen Zahl des Körpers $K(Z)$ erfüllt. Die Anzahl der nach $\mathfrak{p}$ einander inkongruenten Wurzeln dieser Kongruenz ist daher gleich der Anzahl der nach $\mathfrak{p}$ inkongruenten ganzen Zahlen, d. h. gleich der Norm von $\mathfrak{p}$ in $K(Z)$; da nun der Körper

$K(Z)$ vom Relativgrade $f = \frac{m}{e}$ in Bezug auf $k^{(e)}$ ist, so ist $n(\mathfrak{p}) = p^f$; da ferner nach einem Fundamentalsatz aus der Theorie der Kongruenzen die Anzahl der Wurzeln obiger Kongruenz, weil $\mathfrak{p}$ ein Primideal ist, den Grad $p^{f'}$ sicher nicht übersteigt, so ist

$$p^f \leqq p^{f'},$$

d. h.

$$f \leqq f'.$$

Nach dem vorher bewiesenen Satze aber ist, weil $\mathfrak{p}$ ein Primideal ersten Grades von $k^{(e)}$,

$$f' \leqq f.$$

Hieraus folgt, dass genau

$$f' = f$$

sein muss.

Hiermit ist der erste Teil des Satzes bewiesen.

Sei jetzt $\mathfrak{p}'$ ein zu $\mathfrak{p}$ konjugirtes Primideal in $K(Z)$ und vom ersten Grade in $k^{(e')}$, so muss die zu $k^{(e')}$ gehörende Untergruppe mit der zu $k^{(e)}$ gehörenden übereinstimmen, in Folge des vorigen Satzes; also muss $e' = e$ und $k^{(e')}$ identisch mit $k^{(e)}$ sein. Sei also

$$p = \mathfrak{p}_1 \ldots \mathfrak{p}_\varkappa$$

die Zerlegung der rationalen Primzahl p in $K(Z)$, wo $\mathfrak{p}_1, \ldots, \mathfrak{p}_\varkappa$ Primideale ersten Grades in $k^{(e)}$, so ist

$$n(p) = p^{\varkappa \cdot f};$$

andrerseits ist

$$n(p) = p^m;$$

also ist

$$\varkappa \cdot f = m$$

d. h.

$$\varkappa = \frac{m}{f} = e,$$

womit auch der zweite Teil des zweiten Satzes bewiesen ist.

Auf Grund beider Sätze beweisen wir jetzt folgenden **Satz 3**:

Ist f der kleinste positive Exponent der ungeraden rationalen Primzahl p, für welchen $p^f \equiv 1$, (2^λ)

ausfällt, so lautet die Zerlegung von p in Primideale des Körpers $K(Z)$, wie folgt:

$$p = \mathfrak{p}_1 \ldots\ldots \mathfrak{p}_e,$$

wo $\mathfrak{p}_1 \ldots\ldots \mathfrak{p}_e$ von einander verschiedene Primideale f^{ten} Grades von $K(Z)$ und ersten Grades in demjenigen der drei Unterkörper $k^{(e)}$ vom Grade $e = \frac{m}{f}$, dessen bestimmende Zahl bei der Substitution $\sigma = (Z : Z^p)$ ungeändert bleibt.

Beweis. Die Substitutionen $\sigma = (Z : Z^p)$, $\sigma^2 = (Z : Z^{p^2})$, ..., $\sigma^f = (Z : Z^{p^f})$ bilden eine Untergruppe f^{ten} Grades U_f, welche einem Unterkörper $k^{(e)}$ vom Grade $e = \frac{m}{f}$ zugehört. Sei nun $\mathfrak{p}$ ein in p aufgehendes Primideal von $K(Z)$, welches vom ersten Grade in $k^{(e')}$ sei, so muss die Untergruppe, die zu $k^{(e')}$ gehört, mit U_f übereinstimmen und folglich $k^{(e')}$ mit $k^{(e)}$ identisch sein. Dann ergiebt sich aber die Richtigkeit der Behauptung aus dem Beweise des zweiten Teiles des zweiten Satzes.

Wir heben jetzt noch einige aus den eben aufgestellten Sätzen fliessende Korollare hervor.

1. Kennt man irgend eine rationale Primzahl p, welche in einem Unterkörper $k^{(e)}$ in Primideale von $K(Z)$ zerlegt wird, so kennt man auch die zu $k^{(e)}$ gehörende Untergruppe. Dieselbe besteht aus den verschiedenen Potenzen der Substitution $\sigma = (Z : Z^p)$.

2. Die Untergruppen derjenigen Unterkörper, in welchen Primideale von $K(Z)$ liegen, sind sämmtlich cyklische Gruppen.

3. In den reellen Unterkörpern nur, mit Ausnahme des Körpers $K(Z+Z^{-1})$, (Reihe III. § 1.) liegen keine Primideale von $K(Z)$, da nur die zu diesen Unterkörpern gehörenden Untergruppen, ausgenommen diejenige zweiten Grades, sämmtlich nicht cyklisch sind.

4. Um die rationalen Primzahlen hinsichtlich ihrer Zerlegung in Primideale des Körpers $K(Z)$ auf die Unterkörper zu verteilen, lässt sich leicht eine praktische Methode angeben.

In einem nicht cyklischen Unterkörper $k\left(Z^{\frac{m}{e}}\right)$ vom Grade e mögen die rationalen Primzahlen

$$p = 2^\lambda \cdot \varkappa + \nu,$$

wo $\varkappa$ eine positive ganze Zahl, ν eine positive ungerade Zahl unterhalb 2^λ bezeichnet, in Primideale des Körpers $K(Z)$ zerlegt werden. Man kann dann leicht die sämmtlichen verschiedenen Formen rationaler Primzahlen angeben, welche in $k\left(Z^{\frac{m}{e}}\right)$ zerlegt werden. Man bilde sämmtliche nach (2^λ) inkongruente Potenzen von p mit ungeradem Exponenten, nämlich

$$p^1, p^3, p^5, \ldots\ldots, p^{\frac{m}{e}-1};$$

dann sind die sämmtlichen verschiedenen Formen rationaler Primzahlen, $p_1, p_2, p_3, \ldots$, welche in $k\left(Z^{\frac{m}{e}}\right)$ zerlegt werden, durch folgende Kongruenzen festgelegt:

$$\left.\begin{array}{lll} p_1 \equiv p^1, & p_2 \equiv p^3, & p_3 \equiv p^5, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ , & & p_{\frac{m}{2e}} \equiv p^{\frac{m}{e}-1} \end{array}\right\}, \quad (2^\lambda).$$

Aus irgend einer Form, welche in $k\left(Z^{\frac{m}{e}}\right)$ zerlegt wird, kann man sogleich wieder eine Form q erhalten, welche in $k\left(Z^{\frac{m}{2e}}\right)$, dem nichtcyklischen Unterkörper nächsthöheren Grades, in Primideale von $K(Z)$ zerlegt wird; aus p erhält man die Form q durch die Kongruenz

$$q \equiv p^2, \quad (2^\lambda).$$

Bezeichnen dann $q_1, q_2, q_3, \ldots.$ die sämmtlichen verschiedenen Formen, welche in $k\left(Z^{\frac{m}{2e}}\right)$ zerlegt werden, so hat man zur Bestimmung derselben die Kongruenzen:

$$\begin{array}{lll} q_1 \equiv q^1, & q_2 \equiv q^3, & q_3 \equiv q^5 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ , & & q_{\frac{m}{4e}} \equiv q^{\frac{m}{2e}-1}. \end{array}$$

Da nun stets in $k(\sqrt{-1})$ die rationalen Primzahlen

$$p = 2^\lambda \cdot \varkappa + 5$$

zerlegt werden, so kann man successive von diesem Körper zu höheren aufsteigend leicht sämmtliche Formen aufstellen, welche in den nichtcyklischen Unterkörpern (§ 1, Reihe I) zerlegt werden.

Man kann nun auch sofort die Formen aller übrigen Primzahlen, deren Zerlegung abgesehen von $k(Z+Z^{-1})$ auf die imaginären cyklischen Unterkörper (der Reihe II, § 1) beschränkt ist, den einzelnen Unterkörpern zuordnen. Wird in dem Unterkörper $k\left(Z^{\frac{m}{e}}\right)$ die Form $p = 2^{\lambda}\varkappa + \nu$ zerlegt, so wird in dem Unterkörper $k\left(Z^{\frac{m}{2e}} - Z^{-\frac{m}{2e}}\right)$, der von dem gleichen Grade e ist, die Form $p' = 2^{\lambda}\cdot\varkappa - \nu$ zerlegt. Die rationalen Primzahlen von der Form $p = 2^{\lambda}\cdot\varkappa + 1$ werden in Primideale ersten Grades von $K(Z)$, die Form $p = 2^{\lambda}\cdot\varkappa - 1$ wird im Unterkörper $k(Z+Z^{-1})$ in Primideale von $K(Z)$ zerlegt.

Man erhält aus dem Bisherigen das Korollar: Die Anzahl der verschiedenen Formen rationaler Primzahlen, welche in einem Unterkörper in Primideale von $K(Z)$ zerlegt werden, ist stets gleich der halben Anzahl der Substitutionen der dem betreffenden Unterkörper zugehörenden Untergruppe.

Die eindeutige Zerlegung aller Zahlen in Primzahlen ist nicht in jedem Kreiskörper $k\left(e^{\frac{2i\pi}{2^{\lambda}}}\right)$ möglich; doch ist die Anzahl der Idealklassen für jeden dieser Körper eine ungerade, wie H. Weber gezeigt hat. Aus den Tafeln von Reuschle ersieht man, dass in den Körpern der 4ten, 8ten, 16ten, 32ten Einheitswurzeln die Klassenanzahl gleich 1 ist.

§ 4.

Die Bestimmung des quadratischen Charakters einer beliebigen Zahl des Körpers $K\left(e^{\frac{2i\pi}{2^{\lambda}}}\right)$ ist stets zurückführbar auf die Bestimmung des quadratischen Charakters rationaler Zahlen in $k(1)$.

Der quadratische Charakter einer Zahl eines algebraischen Zahlkörpers k wird folgendermassen definirt.

Es sei α eine beliebige Zahl und $\mathfrak{p}$ ein beliebiges zu α primes Primideal des Körpers k, so ist α quadratischer Rest oder Nichtrest nach $\mathfrak{p}$, jenachdem die Kongruenz

$$\alpha \equiv \xi^2, \quad (\mathfrak{p})$$

durch irgend eine Zahl ξ von k befriedigt werden kann oder nicht. In Erweiterung des Legendre'schen Symboles in der Theorie der rationalen Zahlen, wird die symbolische Gleichung

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1$$

dahin definirt, dass α quadratischer Rest nach $\mathfrak{p}$ in k, und

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = -1$$

dahin definirt, dass α quadratischer Nichtrest nach $\mathfrak{p}$ in k ist.

Für das neu definirte Symbol gelten folgende Rechnungsregeln.

1. Sind $\alpha, \beta, \gamma, \ldots$ zu $\mathfrak{p}$ prime Zahlen von k, so ist

$$\left(\frac{\alpha \cdot \beta \cdot \gamma \cdots}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right) \cdot \left(\frac{\beta}{\mathfrak{p}}\right) \cdot \left(\frac{\gamma}{\mathfrak{p}}\right) \cdots$$

2. Ist $\mathfrak{j}$ ein beliebiges zu α primes Ideal von k und

$$\mathfrak{j} = \mathfrak{p} \cdot \mathfrak{q} \cdot \mathfrak{r} \cdots \mathfrak{w},$$

wo $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots \mathfrak{w}$ von einander verschiedene Primideale sind, so ist

$$\left(\frac{\alpha}{\mathfrak{j}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right) \cdot \left(\frac{\alpha}{\mathfrak{q}}\right) \cdot \left(\frac{\alpha}{\mathfrak{r}}\right) \cdots \left(\frac{\alpha}{\mathfrak{w}}\right).$$

Wir beweisen jetzt folgende Kongruenz

$$\left(\frac{\alpha}{\mathfrak{p}}\right) \equiv \alpha^{\frac{n(\mathfrak{p})-1}{2}}, \quad (\mathfrak{p}),$$

wo $n(\mathfrak{p})$ die Norm von $\mathfrak{p}$ in k bezeichnet. Die Kongruenz sagt aus, dass α quadratischer Rest nach $\mathfrak{p}$ ist, wenn $\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv +1, (\mathfrak{p})$ ausfällt, und dass α quadratischer Nichtrest nach $\mathfrak{p}$ ist, wenn $\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv -1, (\mathfrak{p})$ ausfällt.

Sei nun zunächst α Rest nach $\mathfrak{p}$, d. h. $\alpha \equiv \beta^2$, $(\mathfrak{p})$, so ist

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \beta^{n(\mathfrak{p})-1} \equiv +1, \quad (\mathfrak{p}),$$

nach dem Fermat'schen Satze, da α und folglich auch β prim zu $\mathfrak{p}$ ist. Damit ist der erste Teil der Behauptung bewiesen. Wir beweisen den zweiten Teil derselben. Wie der Fermat'sche Satz, so gilt auch in einem beliebigen algebraischen Zahlkörper der Satz von der Existenz der Primitivzahlen nach einem Primzahlmodul. Nach einem Primideale $\mathfrak{p}$ giebt es stets $\varphi(\mathfrak{p}) = n(\mathfrak{p})-1$ Zahlen ϱ, welche die Eigenschaft haben, dass erst ihre $(n(\mathfrak{p})-1)$te Potenz kongruent 1 nach $(\mathfrak{p})$ wird, und dass ferner die sämmtlichen Potenzen von ϱ, von der ersten bis zur $(n(\mathfrak{p})-1)$ten ein vollständiges Restsystem von $n(\mathfrak{p})$ nach $\mathfrak{p}$ inkongruenten Zahlen bilden.

Nehmen wir also an, α sei Nichtrest nach $\mathfrak{p}$, so werden wir setzen dürfen

$$\alpha \equiv \varrho^e, \quad (\mathfrak{p}),$$

wo e jedenfalls eine ungerade Zahl ist. Mithin ist

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \varrho^{e\cdot\frac{n(\mathfrak{p})-1}{2}} \equiv \varrho^{\frac{n(\mathfrak{p})-1}{2}+\frac{e-1}{2}\cdot(n(\mathfrak{p})-1)}, \quad (\mathfrak{p})$$

also

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \varrho^{\frac{n(\mathfrak{p})-1}{2}} \not\equiv +1, \quad (\mathfrak{p}),$$

da erst die $(n(\mathfrak{p})-1)$te Potenz von ϱ kongruent $+1$ nach $\mathfrak{p}$ wird.

Da ferner

$$(\alpha^{n(\mathfrak{p})-1}-1) = \left(\alpha^{\frac{n(\mathfrak{p})-1}{2}}-1\right)\left(\alpha^{\frac{n(\mathfrak{p}-1)}{2}}+1\right) \equiv 0, \quad (\mathfrak{p}),$$

und, wie soeben gezeigt,

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}}-1 \not\equiv 0, \quad (\mathfrak{p})$$

ist, so muss notwendig

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}}+1 \equiv 0, \quad (\mathfrak{p}),$$

oder

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv -1, \quad (\mathfrak{p})$$

sein q. e. d.

Wir legen jetzt als Grundkörper einen Kreiskörper der 2^hten Einheitswurzeln zugrunde und werden zeigen, dass man hier der Kongruenz $\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)$, $(\mathfrak{p})$ eine sehr einfache für die Berechnung geeignete Form erteilen kann.

Es ist bekannt, dass die Berechnung des quadratischen Charakters einer Zahl $f(\omega)$ eines algebraischen Zahlkörpers $k(\omega)$ nach einer Primzahl ersten Grades $\varphi(\omega)$ von k keine Schwierigkeiten bietet. Sei die Norm der Primzahl ersten Grades $n(\varphi(\omega)) = p^1$ und das Ideal $(\varphi(\omega)) = (p, \omega - a)$ gesetzt, wo a irgend eine positive oder negative ganze rationale Zahl bezeichnet, so ist

$$\omega \equiv a, \quad (\varphi(\omega)),$$

und man kann daher auch

$$f(\omega) \equiv r, \quad (\varphi(\omega))$$

setzen, wo r ganz und rational.

Für

$$\left(\frac{f(\omega)}{\varphi(\omega)}\right) \equiv \{f(\omega)\}^{\frac{n(\varphi(\omega))-1}{2}}, \quad (\varphi(\omega))$$

erhält man

$$\left(\frac{f(\omega)}{\varphi(\omega)}\right) \equiv r^{\frac{p-1}{2}}, \quad (p).$$

Nun ist

$$\operatorname{ind} r^{\frac{p-1}{2}} \equiv \frac{p-1}{2} \operatorname{ind} r, \quad (p-1);$$

jenachdem also ind r gerade oder ungerade ausfällt, ist

$$\operatorname{ind} r^{\frac{p-1}{2}} \equiv 0, \ (p-1), \ \text{also } r^{\frac{p-1}{2}} \equiv +1, \ (p)$$

oder

$$\operatorname{ind} r^{\frac{p-1}{2}} \equiv \frac{p-1}{2}, \ (p-1), \ \text{also } r^{\frac{p-1}{2}} \equiv -1, \ (p).$$

Wir untersuchen jetzt im Körper $K(Z)\left(Z = e^{\frac{2i\pi}{2^h}}\right)$ den quadratischen Charakter einer beliebigen Primzahl $f(Z)$ nach einer beliebigen Primzahl $\varphi(Z)$.

Es sei $f(Z)$ eine Primzahl f'ten Grades in $K(Z)$ mit der Norm $n(f(Z)) = q^{f'}$, und vom ersten Grade in dem Unterkörper $k^{(e')}$ dessen Grad gleich $e' = \frac{m}{f'}$, $\varphi(Z)$ sei eine Primzahl $f$ten Grades in $K(Z)$ mit der Norm $n(\varphi(Z)) = p^f$, und vom ersten Grade in dem Unterkörper $k^{(e)}$, dessen Grad gleich $e = \frac{m}{f}$. Hierbei sind die Fälle $f' = 1$, $e' = m$, $f = 1$, $e = m$, $f' = f$, $e' = e$, $f' = f = 1$, $e' = e = m$ nicht ausgeschlossen. Es sei noch bemerkt, dass die Grössen f', f, e', e, m Potenzen von 2 sind.

Es ist

$$\left(\frac{f(Z)}{\varphi(Z)}\right) \equiv (f(Z))^{\frac{p^f-1}{2}}, \quad (\varphi(Z))$$

$$\equiv \left\{f(Z)^{1+p+p^2+\cdots+p^{f-1}}\right\}^{\frac{p-1}{2}}, \quad (\varphi(Z))$$

$$\equiv \left\{f(Z)\cdot f(Z)^p\cdots f(Z)^{p^{f-1}}\right\}^{\frac{p-1}{2}}, \quad (\varphi(Z)).$$

Nach einem bekannten Satze aus der Theorie der Kongruenzen ist

$$f(Z)^p \equiv f(Z^p), \quad (p),$$

folglich

$$f(Z)^{p^2} \equiv f(Z^{p^2}), \quad (p),$$

$$f(Z)^{p^3} \equiv f(Z^{p^3}), \quad (p)$$

$$\cdots\cdots\cdots\cdots$$

$$f(Z)^{p^{f-1}} \equiv f(Z^{p^{f-1}}), \quad (p).$$

Diese Kongruenzen werden a fortiori nach dem Modul $\varphi(Z)$ bestehen, wir dürfen also setzen

$$\left(\frac{f(Z)}{\varphi(Z)}\right) \equiv \left\{f(Z)\cdot f(Z^p)\cdots f(Z^{p^{f-1}})\right\}^{\frac{p-1}{2}}, \quad (\varphi(Z)).$$

Jetzt werden wir beweisen, dass das Produkt in geschwungener Klammer gleich der Relativnorm der Primzahl $f(Z)$ in Bezug auf den Unterkörper $k^{(e)}$ im Körper $K(Z)$ als Relativkörper hinsichtlich $k^{(e)}$ ist. Der Relativgrad von $K(Z)$ in Bezug auf $k^{(e)}$

ist $\frac{m}{e} = f$. Die Gleichung niedrigsten Grades, welcher Z genügt und deren Koëfficienten in $k^{(e)}$ liegen, wird also folgende Form besitzen

$$F(Z) = Z^f + \alpha_1 Z^{f-1} + \cdots + \alpha_f = 0.$$

Sind die Koëfficienten dieser Gleichung nur als Funktionen von Z gegeben, so ist die Gleichung eine Identität in Z, d. h. sie besteht für jeden Wert von Z. Substituirt man der Reihe nach Z^p für Z, Z^{p^2} für $Z, \ldots Z^{p^{f-1}}$ für Z, so bleiben die Koëfficienten $\alpha_1 \ldots \alpha_f$ dieselben Funktionen von Z, da sie Zahlen in $k^{(e)}$ sind und daher bei den Substitutionen der Untergruppe, die zu $k^{(e)}$ gehört, ungeändert bleiben und man erhält daher folgende Gleichungen

$$\begin{gathered}
(Z^p)^f + \alpha_1 (Z^p)^{f-1} + \cdots + \alpha_f = 0 \\
(Z^{p^2})^f + \alpha_1 (Z^{p^2})^{f-1} + \cdots + \alpha_f = 0 \\
\cdots\cdots\cdots\cdots \\
(Z^{p^{f-1}})^f + \alpha_1 (Z^{p^{f-1}})^{f-1} + \cdots + \alpha_f = 0.
\end{gathered}$$

Die zu Z relativ conjugirten Wurzeln der Gleichung $F(Z) = 0$ sind also $Z^p, Z^{p^2}, \ldots Z^{p^{f-1}}$. Der Körper $K(Z)$ ist ein relativ-Abelscher in Bezug auf jeden seiner Unterkörper. Man erkennt jetzt auch, dass die Koëfficienten der Relativgleichung für Z ganze Zahlen in $k^{(e)}$ sind; denn, da sie die elementarsymmetrischen Funktionen von $Z, Z^p, \ldots Z^{p^{f-1}}$ sind, so sind sie zunächst ganze Zahlen in $K(Z)$; da sie aber Zahlen in $k^{(e)}$ sind, so müssen sie auch ganze Zahlen in $k^{(e)}$ sein [1]).

Es ist jetzt leicht zu beweisen, dass $f(Z)$, sowie jede ganze Zahl in $K(Z)$, folgende identische Umformung gestattet

$$f(Z) = \gamma_1 + \gamma_2 Z + \gamma_3 Z^2 + \cdots + \gamma_f Z^{f-1},$$

wo $\gamma_1, \gamma_2 \ldots \gamma_f$ ganze Zahlen in $k^{(e)}$ sind, die zum Teil verschwinden können. Es ist dann

1) Dieser Satz ist in der Theorie des Relativkörpers das Analogon des Satzes: Wenn eine ganze algebraische Zahl zugleich rational ist, so ist sie eine ganze rationale Zahl.

$$f(Z^p) = \gamma_1 + \gamma_2 Z^p + \gamma_3 (Z^p)^2 + \cdots + \gamma_f (Z^p)^{f-1}$$

$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$

$$f(Z^{p^{f-1}}) = \gamma_1 + \gamma_2 (Z^{p^{f-1}}) + \gamma_3 (Z^{p^{f-1}})^2 + \cdots + \gamma_f (Z^{p^{f-1}})^{f-1}.$$

Also ist das Produkt

$$f(Z) \cdot f(Z^p) \cdots\cdots f(Z^{p^{f-1}})$$

die Relativnorm von $f(Z)$ in Bezug auf $k^{(e)}$ und mithin eine ganze Zahl in $k^{(e)}$. Denn $f(Z)$ genügt auch einer Gleichung f^{ten} Grades mit Koëfficienten in $k^{(e)}$. Die Wurzeln dieser Gleichung, die man aus $F(Z)$ durch die Tschirnhausen-Transformation erhält und die im Allgemeinen reducibel sein wird, sind $f(Z)$, $f(Z^p)$, $\ldots f(Z^{p^{f-1}})$. Das Produkt aller Wurzeln ist gleich dem letzten Koëfficienten dieser Gleichung, also eine Zahl in $k^{(e)}$.

Man kann hier aber auch unmittelbar erkennen, dass das Produkt $f(Z) \cdot f(Z^p) \ldots . f(Z^{p^{f-1}})$ eine Zahl in $k^{(e)}$ ist, da es bei der Substitution $\sigma = (Z : Z^p)$ in das wegen $Z^{p^f} = Z$ identische Produkt $f(Z^p) \cdot f(Z^{p^2}) \ldots . f(Z^{p^f})$ übergeht.

Das Resultat, zu welchem wir zunächst gelangt sind, lautet, wie folgt:

Satz 4. *Der quadratische Charakter von $f(Z)$ nach $\varphi(Z)$ in $K(Z)$ ist identisch mit dem quadratischen Charakter, welchen im Körper $k^{(e)}$ die Relativnorm $N_{k^{(e)}}(f(Z))$ von $f(Z)$ in Bezug auf $k^{(e)}$ nach $\varphi(Z)$ besitzt.*

$$\left(\frac{f(Z)}{\varphi(Z)}\right) \equiv \left(N_{k^{(e)}}(f(Z))\right)^{\frac{p-1}{2}}, \quad (\varphi(Z)).$$

Wir beweisen jetzt einen Satz über die Relativnorm $N_{k^{(e)}}(f(Z))$, auf Grund dessen eine unendliche Anzahl reciproker Beziehungen $\left(\frac{f(Z)}{\varphi(Z)}\right) = \left(\frac{\varphi(Z)}{f(Z)}\right)$ im Kreiskörper $K(Z)$ als a priori gegeben erscheint.

Die zu $k^{(e')}$ bezw. $k^{(e)}$ gehörenden Untergruppen, die mit $U_{f'}$ bezw. U_f bezeichnet seien, mögen g Substitutionen gemeinsam haben, dann werden diese g Substitutionen wieder eine Untergruppe vom Grade g bilden, die zu einem Unterkörper $k^{(e'')}$ vom Grade $e'' = \dfrac{m}{g}$

gehören; $k^{(d)}$ wird dann der Oberkörper niedrigsten Grades sein, der $k^{(e')}$ und $k^{(e)}$ als Unterkörper enthält.

Es ist für das Folgende gleichgültig, ob wir $f \leqq f'$ oder $f' \leqq f$ voraussetzen. Indem wir das Letztere annehmen, werden wir jedenfalls das Ungleichungssystem

$$1 \leqq g \leqq f' \leqq f$$

aufstellen müssen; denn wenigstens eine Substitution, nämlich die identische, haben stets zwei Untergruppen gemeinsam und g kann jedenfalls nicht grösser als sein.

Mit Berücksichtigung dessen, dass g, f', f stets Potenzen von 2 sind, stellen wir noch, indem wir $g = 2^{\varkappa}$, $f' = 2^{\nu}$, $f = 2^{\mu}$ setzen, die Ungleichungen

$$0 \leqq \varkappa \leqq \nu \leqq \mu$$

auf. Wir beweisen jetzt folgenden **Satz 5.**

Die Relativnorm $N_{k^{(e)}}(f(Z))$ ist gleich der g^{ten} Potenz einer durch $f(Z)$ teilbaren Primzahl des Körpers $k^{(e)}$, deren Grad in $k^{(e)}$ gleich $\frac{f'}{g}$ ist.

Beweis. Es ist

$$N_{k^{(e)}}(f(Z)) = f(Z) \cdot f(Z^{p}) \cdot f(Z^{p^2}) \ldots f(Z^{p^{f-1}}).$$

Ist $g > 1$ so werden die Zahlen $f(Z^{p})$, $f(Z^{p^2})$, $f(Z^{p^3}) \ldots f(Z^{p^{f-1}})$ nicht sämmtlich von $f(Z)$ verschieden sein. Ist in der Reihe dieser Zahlen $f(Z^{p^r})$ die erste, welche gleich $f(Z)$ wird, so wird auch

$$f(Z^{p^{2r}}) = f(Z)$$
$$f(Z^{p^{3r}}) = f(Z)$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$f(Z^{p^{gr}}) = f(Z).$$

Ferner

$$f(Z^{p^{r+1}}) = f(Z^{p})$$
$$f(Z^{p^{r+2}}) = f(Z^{p^2})$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$f(Z^{p^{2r-1}}) = f(Z^{p^{r-1}})$$

und weiter

$$f(Z^{p^{2F+1}}) = f(Z^p)$$
$$f(Z^{p^{2F+2}}) = f(Z^{p^2})$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

woraus man ersieht, dass

$$f(Z)\cdot f(Z^p)\dots f(Z^{p^{f-1}})$$
$$= \{f(Z)\cdot f(Z^p)\dots f(Z^{p^{F-1}})\}^g (f(Z)\dots . f(Z^{p^{F'-1}})),$$

wo $F' < F$, falls $g \cdot F \neq f$. Alsdann bleibt aber die linke Seite dieser Gleichung nicht ungeändert bei der Substitution $\sigma = (Z : Z^p)$. Es muss also

$$g \cdot F = f$$

sein, d. h. es ist

$$N_{k^{(o)}}(f(Z)) = \{f(Z)\cdot f(Z^p)\dots f(Z^{p^{F-1}})\}^g.$$

Bezeichnen wir jetzt das Produkt in geschwungener Klammer mit $r(Z)$, so wird die Norm $\nu(r(Z))$ von $r(Z)$ im Körper $k^{(o)}$ eine gewisse Potenz der rationalen Primzahl q sein, da $f(Z)$ ein Primfaktor von q in $K(Z)$ ist; wir setzen

$$\nu(r(Z)) = q^d.$$

Mithin ist, wenn mit $n(f(Z))$ die Norm $q^{f'}$ von $f(Z)$ in $K(Z)$ bezeichnet wird,

$$\nu(r(Z)^g) = q^{g \cdot d} = n(f(Z)) = q^{f'},$$

woraus folgt $g \cdot d = f'$, $d = \dfrac{f'}{g}$.

Hiermit ist unser Satz bewiesen.

Das Resultat ist in Formeln:

$$\left(\frac{f(Z)}{\varphi(Z)}\right) \equiv (r(Z)^g)^{\frac{p-1}{2}}, \quad (\varphi(Z));$$

Hier ist $r(Z)^g = N_{k^{(o)}}(f(Z))$, $r(Z)$ eine durch $f(Z)$ teilbare Primzahl vom Grade $d = \dfrac{f'}{g}$ des Körpers $k^{(o)}$.

Hieraus folgt, dass, wenn $g > 1$, also gewiss $g \equiv 0$, (2) ist,

$$\left(\frac{f(Z)}{\varphi(Z)}\right) \equiv \left(r(Z)^{\frac{g}{2}}\right)^{p-1} \equiv +1, \quad (\varphi(Z)).$$

Ferner ist

$$\left(\frac{\varphi(Z)}{f(Z)}\right) \equiv (R(Z)^g)^{\frac{p-1}{2}}, \quad (f(Z)),$$

wo $R(Z)^g = N_{k^{(e')}}(\varphi(Z))$, d. h. gleich der Relativnorm von $\varphi(Z)$ in Bezug auf den Unterkörper $k^{(e')}$ von $K(Z)$, $R(Z)$ eine Primzahl vom Grade $D = \frac{f}{g}$ des Körpers $k^{(e')}$. Ist also $g > 1$, d. h. $g \equiv 0$, (2), so wird

$$\left(\frac{\varphi(Z)}{f(Z)}\right) \equiv \left(R(Z)^{\frac{g}{2}}\right)^{p-1} \equiv +1, \quad (f(Z));$$

Wir sprechen jetzt folgenden **Satz 6** aus:

Sind $f(Z)$ und $\varphi(Z)$ Primzahlen von $K(Z)$, welche bezw. in $k^{(e')}$ und $k^{(e)}$ vom ersten Grade sind, und haben die zu $k^{(e')}$ und $k^{(e)}$ gehörenden Untergruppen $U_{f'}$ und U_f mehr als eine Substitution gemeinsam, so ist im Körper $K(Z)$

$$\left(\frac{f(Z)}{\varphi(Z)}\right) = \left(\frac{\varphi(Z)}{f(Z)}\right) = +1.$$

§ 5.

Die Einheiten des Kreiskörpers der $2^{h\text{ten}}$ Einheitswurzeln.

Nach einem von Kronecker zuerst aufgestellten Satze über die Einheiten in Kreiskörpern gilt im Besonderen für die Kreiskörper der $2^{h\text{ten}}$ Einheitswurzeln $K\left(e^{\frac{2i\pi}{2^h}}\right) = K(Z)$ folgende Thatsache: Eine jede beliebige Einheit η des Kreiskörpers $K(Z)$ ist folgendermassen darstellbar

$$\eta = Z^n \cdot \varepsilon,$$

wo ε eine reelle im Körper $K(Z)$ liegende Einheit und Z^n eine Potenz der Einheitswurzel Z mit ganzzahligem Exponenten bezeichnen.

Was die reellen Einheiten des Körpers $K(Z)$ anbetrifft, so springt sogleich ein System von $\frac{m}{2}$ konjugirten Einheiten in's Auge, welche in dem reellen Unterkörper $k(Z+Z^{-1})$ liegen. Bezeichnet man die den Unterkörper $k(Z+Z^{-1})$ definirende Gleichung mit

$$\varphi(x) = 0,$$

die Wurzeln dieser Gleichung, welche vom Grade $\frac{m}{2}$ ist, mit

$$\zeta_1, \zeta_2, \zeta_3, \ldots, \zeta_{\frac{m}{2}},$$

so gilt identisch in x die Gleichung

$$\varphi(x) = (x-\zeta_1)(x-\zeta_2)(x-\zeta_3)\ldots.\left(x-\zeta_{\frac{m}{2}}\right);$$

setzt man $x = 1$, so erhält man stets

$$(1-\zeta_1)(1-\zeta_2)(1-\zeta_3)\ldots\left(1-\zeta_{\frac{m}{2}}\right) = \varphi(1) = -1.$$

Die Zahlen $1-\zeta_1$, $1-\zeta_2$, $1-\zeta_3$, $\ldots$, $1-\zeta_{\frac{m}{2}}$ sind also offenbar Einheiten, da die Norm jeder derselben im Körper $k(Z+Z^{-1})$ gleich -1 ist.

Beliebige $\frac{m}{2}-1$ dieser Einheiten sind also von einander unabhängig, und da die Anzahl der Grundeinheiten des Körpers $K(Z)$, der nebst seinen sämmtlichen konjugirten Körpern imaginär ist, ebenfalls gleich $\frac{m}{2}-1$ ist nach dem Dirichlet'schen Fundamentalsatze über die Einheiten des algebraischen Zahlkörpers, so sollen die genannten Einheiten, also beliebige $\frac{m}{2}-1$ der $\frac{m}{2}$ Einheiten $1-\zeta_1$, $1-\zeta_2$, $1-\zeta_3$, $\ldots$, $1-\zeta_{\frac{m}{2}}$, die mit $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots \varepsilon_{\frac{m}{2}}$ bezeichnet werden mögen, zunächst hypothetisch als Grundeinheiten angenommen werden, wonach dann jede beliebige Einheit η des Körpers $K(Z)$ in der Form

$$\eta = Z^{n} \cdot \varepsilon_1^{n_1} \cdot \varepsilon_2^{n_2} \cdot \varepsilon_3^{n_3} \cdots \varepsilon_{\frac{m}{2}-1}^{n_{\frac{m}{2}-1}}$$

darstellbar ist, wo $n, n_1, n_2, \ldots, n_{\frac{m}{2}-1}$ irgend welche ganze positive oder negative Zahlen oder Null bezeichnen.

In jedem einzelnen Falle, wo wir uns im Folgenden der hier abgeleiteten Einheiten zum Zwecke der Bestätigung des Reciprocitätsgesetzes bedienen werden, werden wir entweder zeigen, dass diese Einheiten Grundeinheiten sind, oder wenigstens dies, dass dieselben sich von den Grundeinheiten, wenn überhaupt, dann nur um einen quadratischen Einheitsfaktor unterscheiden.

§ 6.

Das allgemeine quadratische Reciprocitätsgesetz.

Wir geben hier das allgemeine quadratische Reciprocitätsgesetz nach § 3 der Abhandlung über die Theorie der relativ-Abel'schen Zahlkörper.

Zugrunde liegen folgende beiden Voraussetzungen:

1 Der algebraische Zahlkörper k vom m^{ten} Grade sei nebst allen konjugirten Körpern $k', k'', \ldots, k^{(m-1)}$ imaginär.

2. Die Anzahl h der Idealklassen im Körper k sei gleich 1. .

Dem ersten Ergänzungssatze liegen folgende beiden Definitionen zugrunde:

Definition 1. „Ein solches zu 2 primes Ideal $\mathfrak{a}$ des Körpers k, in Bezug auf das für jede Einheit ξ in k

$$\left(\frac{\xi}{\mathfrak{a}}\right) = +1$$

ausfällt, heisse ein primäres Ideal".

Definition 2. „Eine solche zu 2 prime ganze Zahl des Körpers k, welche kongruent dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 ausfällt, heisse eine primäre Zahl des Körpers k".

Satz 1. (Erster Ergänzungssatz.)

„Wenn $\mathfrak{a}$ ein primäres Ideal in k ist, so giebt es

stets eine primäre Zahl α, sodass $\mathfrak{a} = (\alpha)$ wird, und umgekehrt: wenn α eine primäre Zahl in k ist, so ist das Ideal $\mathfrak{a} = (\alpha)$ stets ein primäres Ideal".

Wir zerlegen nun die Zahl 2 im Körper k in Primideale wie folgt:

$$2 = \mathfrak{l}_1^{l_1} \cdot \mathfrak{l}_2^{l_2} \cdots \mathfrak{l}_s^{l_s},$$

wo $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_s$ von einander verschiedene Primfaktoren der Zahl 2 in k und $l_1, l_2, \ldots, l_s$ die Potenzexponenten bedeuten, zu denen bez. jene Primideale in der Zahl 2 aufgehen.

Dem zweiten Ergänzungssatze liegen folgende beiden Definitionen 3 und 4 zugrunde:

Definition 3. Ein solches zu 2 primes Ideal $\mathfrak{a}$ des Körpers k, in Bezug auf das nicht nur für jede Einheit ξ in k, sondern auch für jede in 2 aufgehende ganze Zahl λ des Körpers k

$$\left(\frac{\xi}{\mathfrak{a}}\right) = +1, \quad \left(\frac{\lambda}{\mathfrak{a}}\right) = +1$$

ausfällt, heisse ein hyperprimäres Ideal".

Definition 4. „Eine solche zu 2 prime Zahl α des Körpers k, welche kongruent dem Quadrat einer ganzen Zahl in k nach dem Modul

$$\mathfrak{l}_1^{2l_1+1} \cdot \mathfrak{l}_2^{2l_2+1} \cdots \mathfrak{l}_s^{2l_s+1}$$

ausfällt, heisse eine hyperprimäre Zahl des Körpers k".

Satz 2. (Zweiter Ergänzungssatz.)

„Wenn $\mathfrak{a}$ ein hyperprimäres Ideal in k ist, so giebt es stets eine hyperprimäre Zahl α, sodass $\mathfrak{a} = (\alpha)$ wird, und umgekehrt: wenn α eine hyperprimäre Zahl in k ist, so ist das Ideal $\mathfrak{a} = (\alpha)$ stets ein hyperprimäres Ideal".

Satz 3. (Das allgemeine quadratische Reciprocitätsgesetz.)

„Wenn ν, μ, ν', μ' irgend welche zu 2 prime ganze Zahlen in k sind, derart dass die beiden Produkte $\nu \cdot \nu'$ und $\mu \cdot \mu'$ primär ausfallen, so ist stets

$$\left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu'}{\mu'}\right)\left(\frac{\mu'}{\nu'}\right)\text{“}.$$

Aus **Satz 3** ergiebt sich das Korollar:

Sind ν, μ ganze zu 2 prime Zahlen des Körpers k und ist mindestens eine der Zahlen ν, μ primär, so ist

$$\left(\frac{\nu}{\mu}\right) = \left(\frac{\mu}{\nu}\right).$$

§ 7.

Erste Bestätigung in $k\left(e^{\frac{2i\pi}{4}}\right)$.

Die Bestätigung des Reciprocitätsgesetzes in $k(\sqrt{-1}) = k\left(e^{\frac{2i\pi}{4}}\right)$ erscheint zwar als trivialer Fall, lässt sich aber in der umfassendsten Weise ausführen.

Nach § 3 kommen hier zwei Formen rationaler Primzahlen $p = 4n+1$ und $p = 4n+3$ in Betracht, deren Primfaktoren Primzahlen verschiedener Grade sein müssen. Die Primfaktoren der rationalen Primzahlen $p = 4n+1$ sind notwendig vom ersten Grade in $k(\sqrt{-1})$, da allgemein die rationalen Primzahlen $p = 2^h \cdot x + 1$ im Zahlkörper $k\left(e^{\frac{2i\pi}{2^h}}\right)$ in Primideale ersten Grades zerlegt werden. Da ferner der Körper $k(\sqrt{-1})$ als einzigen Unterkörper denjenigen der rationalen Zahlen $k(1)$ besitzt, so müssen die rationalen Primzahlen $p = 4n+3$ selbst Primzahlen in $k(\sqrt{-1})$ sein.

$i = \sqrt{-1}$ ist eine Einheit des Körpers, durch deren Potenzen die drei übrigen $-i, +1, -1$ erhalten werden. Die Relativnorm von i in Bezug auf den einzigen Unterkörper $k(1)$ ist $N_{k(1)}(i) = +1$. Es ist daher zunächst

$$\left(\frac{i}{p}\right) \equiv \left(N_{k(1)}(i)\right)^{\frac{p-1}{2}}, \quad (p)$$

wo $p = 4n+3$, d. h. es ist

$$\left(\frac{i}{p}\right) = +1.$$

In Bestätigung des ersten Ergänzungssatzes ist

$$p = 4n+3 \equiv i^2, \quad (2^2).$$

Bezeichnet man nun mit ω die Primzahlen ersten Grades von $k(\sqrt{-1})$, welche also Primfaktoren der rationalen Primzahlen $p = 4n+1$ sind, so hat man

$$\left(\frac{i}{\omega}\right) \equiv (i)^{\frac{p-1}{2}}, \quad (\omega).$$

Nun ist

$$(i)^{\frac{p-1}{2}} = \sqrt{i}^{\,p-1}.$$

Da nun im Körper $k(\sqrt{i}) = k\left(e^{\frac{2i\pi}{8}}\right)$ die rationalen Primzahlen $p = 8n+1$ in Primzahlen ersten Grades zerlegt werden, so ist

$$\sqrt{i}^{\,p} = \sqrt{i} \text{ für } p = 8n+1,$$

d. h.

$$\sqrt{i}^{\,p-1} = +1.$$

Da ferner die rationalen Primzahlen $p = 4n+1 = 8n+5$ in $k(\sqrt{i})$ in solche Primzahlen zerlegt werden, welche im Unterkörper $k(\sqrt{-1})$ liegen und da $k(\sqrt{i})$ relativ quadratisch in Bezug auf $k(\sqrt{-1})$ ist und die Relativsubstitution $\sigma = (\sqrt{i} : \sqrt{i}^{\,p})$ für $p = 8n+5$ ist, so wird

$$\sqrt{i}^{\,p} = -\sqrt{i} \text{ für } p = 8n+5,$$

d. h.

$$\sqrt{i}^{\,p-1} = -1.$$

Das Resultat ist daher

$$\left(\frac{i}{\omega}\right) = +1 \text{ für } n(\omega) = p = 8n+1,$$

$$\left(\frac{i}{\omega}\right) = -1 \text{ für } n(\omega) = p = 8n+5,$$

wo $n(\omega)$ die Norm von ω in $k(\sqrt{-1})$ ist.

In Bestätigung des ersten Ergänzungssatzes zeigt sich, dass überhaupt alle Zahlen $a+bi$, deren Normen $a^2+b^2 \equiv 1$, (8) ausfallen, unter einer der beiden folgenden Formen enthalten sind

$$(4n \pm 1) \pm 4mi$$
$$4m \pm (4n \pm 1)i,$$

welche Formen irgend einer der Einheiten $+1$, -1, $+i$, $-i$ nach (2^2) kongruent und daher mit einer geeigneten Einheit multipliciert kongruent $+1$ ausfallen.

Hiermit ist der erste Ergänzungssatz in $k(\sqrt{-1})$ vollständig bestätigt. Fast ebenso vollständig wird der zweite Ergänzungssatz bestätigt werden.

Die Primzerlegung der 2 in $k(\sqrt{-1})$ ist

$$2 = i(1-i)^2.$$

Eine primäre Primzahl p bzw. ω wird hyperprimär sein, wenn

$$\left(\frac{1-i}{p}\right) = +1, \text{ bzw. } \left(\frac{1-i}{\omega}\right) = +1,$$

oder wenn

$$p \equiv \alpha^2, (2^2(1-i)) \text{ bzw. } \omega \equiv \beta^2, (2^2(1-i))$$

ausfällt, wo α, β ganze Zahlen in $k(\sqrt{-1})$. Die Relativnorm von $1-i$ in Bezug auf den Körper der rationalen Zahlen ist

$$N_{k(1)}(1-i) = 2.$$

Also ist

$$\left(\frac{1-i}{p}\right) \equiv 2^{\frac{p-1}{2}} \quad (p) \text{ für } p = 4n+3.$$

Wir beweisen, dass

$$\left(\frac{1-i}{p}\right) = +1 \text{ für } p = 8n+7$$

$$\left(\frac{1-i}{p}\right) = -1 \text{ für } p = 8n+3,$$

wo die beiden Formen $8n+7$ und $8n+3$ zusammen in der Form $4n+3$ enthalten sind.

Zunächst ist $2^{\frac{p-1}{2}} = \sqrt{2}^{p-1}$. Nun ist $\sqrt{2} = \sqrt{i} + \sqrt{i}^{-1}$ die bestimmende Zahl des reellen quadratischen Unterkörpers von $k(\sqrt{i})$. In $k(\sqrt{i})$ sind aber die Primfaktoren der rationalen Primzahlen $p = 8n+7$ vom ersten Grade in $k(\sqrt{2})$; daher ist

$$\sqrt{2}^p = \sqrt{2} \text{ für } p = 8n+7.$$

Ferner werden in $k(\sqrt{i})$ die rationalen Primzahlen $p = 8n+3$ im Unterkörper $k(\sqrt{-2})$ zerlegt; daher verwandelt die Substitution $\sigma = (\sqrt{i} : \sqrt{i}^p)$ für $p = 8n+3$ die Zahl $\sqrt{2} = \sqrt{i} + \sqrt{i}^{-1}$ in die konjugirte $-\sqrt{2}$, d. h. es ist

$$\sqrt{2}^p = -\sqrt{2} \text{ für } p = 8n+3.$$

In Bestätigung des zweiten Ergänzungssatzes ist

$$p = 8n+7 \equiv i^2, \quad (2^2(1-i))$$

da sogar

$$8n+7 \equiv i^2, \quad (8).$$

Folgende primäre Primzahlen ω sollen in Bezug auf den hyperprimären Charakter untersucht werden.

$$\omega_{17} = 1+4i, \quad \omega_{41} = 5-4i, \quad \omega_{73} = 3+8i,$$
$$\omega_{89} = 5+8i, \quad \omega_{97} = 9-4i, \quad \omega_{113} = 7-8i,$$

wo der ω beigeschriebene Index hier, wie auch später, diejenige rationale Primzahl bezeichnet, in welcher die Primzahl ω aufgeht. Da

$$\left(\frac{1-i}{\omega}\right) \equiv (1-i)^{\frac{p-1}{2}}, \quad (\omega),$$

so ersetzen wir i und sodann $1-i$ durch die nach ω kongruente rationale Zahl. Man findet in den Täfeln

$$\begin{array}{llll} i \equiv +4 & \text{und daher} & 1-i \equiv 14, & (17) \\ i \equiv -9 & \text{„} \quad \text{„} & 1-i \equiv 10, & (41) \\ i \equiv +27 & \text{„} \quad \text{„} & 1-i \equiv 47, & (73) \\ i \equiv -34 & \text{„} \quad \text{„} & 1-i \equiv 35, & (89) \\ i \equiv -22 & \text{„} \quad \text{„} & 1-i \equiv 23, & (97) \\ i \equiv +15 & \text{„} \quad \text{„} & 1-i \equiv 99, & (113). \end{array}$$

Nach den entsprechenden Moduln findet man die Indices:

$$\begin{array}{lll} \text{ind } 14 = 17, & \text{ind } 10 = 8, & \text{ind } 47 = 31, \\ \text{ind } 35 = 25, & \text{ind } 23 = 79, & \text{ind } 99 = 68. \end{array}$$

Hier sind zwei gerade Indices 8, 68 vorhanden; darnach ist

$$\left(\frac{1-i}{\omega_{41}}\right) = +1, \quad \left(\frac{1-i}{\omega_{113}}\right) = +1.$$

In Bestätigung des zweiten Ergänzungssatzes ist

$$\begin{array}{ll} \omega_{41} = 5-4i \equiv 1, & (2^2(1-i)) \\ \omega_{113} = 7-8i \equiv i^2, & (2^2(1-i)). \end{array}$$

Wir bestätigen jetzt den Satz 3 des Reciprocitätsgesetzes in $k(\sqrt{-1})$, indem wir aus diesem Satze das quadratische Reciprocitätsgesetz, so wie es Gauß in der zweiten Abhandlung über die Theorie der biquadratischen Rest ausgesprochen hat, folgern.

Der Satz 3 besagt offenbar, dass das Vorzeichen, welches durch das Produkt

$$\left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right)$$

bestimmt ist, sich lediglich darnach richtet, wie die Zahlen ν', μ' sich in Bezug auf den Modul 4 verhalten. Im Körper $k(\sqrt{-1})$ ist die Anzahl aller nach 4 inkongruenten und zu 4 primen Reste

$$\varphi(4) = n(4)\left(1 - \frac{1}{n(1-i)}\right),$$

wo $n(4)$ und $n(1-i)$ die Normen von 4 und $1-i$ in $k(\sqrt{-1})$ bezeichnen; es ist daher

$$\varphi(4) = 16(1-\tfrac{1}{2}) = 8.$$

Seien jetzt durch die Zahlen

$$\nu_1,\ \nu_2,\ \nu_3,\ \nu_4,\ \nu_5,\ \nu_6,\ \nu_7,\ \nu_8,\quad \text{I.}$$
$$\mu_1,\ \mu_2,\ \mu_3,\ \mu_4,\ \mu_5,\ \mu_6,\ \mu_7,\ \mu_8,\quad \text{II.}$$

zwei verschiedene Systeme nach 4 inkongruenter und zu 4 primer Reste bezeichnet, und seien ferner sämmtliche 64 durch

$$\left(\frac{\nu_\iota}{\mu_\lambda}\right)\left(\frac{\mu_\lambda}{\mu_\iota}\right)$$

bestimmte Vorzeichen bekannt, wo in den Symbolen jeder der Werte $1, 2, \ldots 8$ von ι mit jedem der Werte $1, 2, \ldots 8$ von λ kombinirt ist, so wird, wenn ν, μ beliebige gegebene Zahlen von $k(\sqrt{-1})$ sind, das durch

$$\left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right)$$

bestimmte Vorzeichen aus den bekannten durch

$$\left(\frac{\nu_\iota}{\mu_\lambda}\right)\left(\frac{\mu_\lambda}{\nu_\iota}\right)$$

bestimmten Vorzeichen, sofort anzugeben sein; denn ist

$$\nu \equiv \nu_\iota,\quad \mu \equiv \mu_\lambda \quad (2^2),$$

so hat man sogleich

$$\left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu_\iota}{\mu_\lambda}\right)\left(\frac{\mu_\lambda}{\nu_\iota}\right),$$

da

$$\nu\cdot\nu_\iota \equiv \nu_\iota^2,\quad \mu\cdot\mu_\lambda \equiv \mu_\lambda^2,\quad (2^2)$$

ausfällt.

Dieser Gedanke liegt der Berechnung des folgenden Schemas zugrunde, bei dessen Betrachtung die Uebereinstimmung des Satzes 3 mit dem von Gauß aufgestellten Satze sogleich in's Auge springt.

Das Vorzeichen, welches in dem Schema durch die λ^{te} Horizontalreihe und die ι^{te} Vertikalreihe bestimmt wird, ist das Vorzeichen: $\left(\frac{\nu_\iota}{\mu_\lambda}\right)\left(\frac{\mu_\lambda}{\nu_\iota}\right)$.

Es ist ferner $\nu_1 \equiv \mu_1$, $\nu_2 \equiv \mu_2, \ldots$ etc. (4), woraus folgt, dass das Schema symmetrisch in Bezug auf die Diagonale von links oben nach rechts unten ist.

	$\nu_1 = 2+i$	$\nu_2 = 1+2i$	$\nu_3 = 2+3i$	$\nu_4 = 3+2i$	$\nu_5 = 4+i$	$\nu_6 = 1+4i$	$\nu_7 = 8+3i$	$\nu_8 = 3+8i$
$\mu_1 = 6+5i$	+1	−1	+1	−1	−1	+1	−1	+1
$\mu_2 = 5+6i$	−1	+1	−1	+1	−1	+1	−1	+1
$\mu_4 = 2+7i$	+1	−1	+1	−1	−1	+1	−1	+1
$\mu_4 = 7+2i$	−1	+1	−1	+1	−1	+1	−1	+1
$\mu_5 = 8+5i$	−1	−1	−1	−1	+1	−1	+1	−1
$\mu_6 = 5+8i$	+1	+1	+1	+1	−1	+1	+1	+1
$\mu_7 = 8+7i$	−1	−1	−1	−1	+1	+1	+1	+1
$\mu_8 = 7+8i$	+1	+1	+1	+1	−1	+1	+1	+1

Wenn also ν_ι eine der Zahlen

$$\text{I}^{\text{a}} \quad \nu_2 \quad \nu_4 \quad \nu_6 \quad \nu_8$$

und μ_λ eine der Zahlen

$$\text{II}^{\text{a}} \quad \mu_2 \quad \mu_4 \quad \mu_6 \quad \mu_8$$

ist, so ist stets

$$\left(\frac{\nu_\iota}{\mu_\lambda}\right)\left(\frac{\mu_\lambda}{\nu_\iota}\right) = +1, \text{ d. h. } \left(\frac{\nu_\iota}{\mu_\lambda}\right) = \left(\frac{\mu_\lambda}{\nu_\iota}\right).$$

Die Zahlen I^{a} und ebenso die Zahlen II^{a} stellen sämmtliche nach (4) inkongruente Reste dar, welche von der Form $(2n+1) \pm 2mi$ sind, einer Form, die stets prim zu 2 ist.

Folglich werden alle Zahlen ν, μ, von dieser Form irgend einer der Zahlen I^{a} oder, was dasselbe ist, einer der Zahlen II^{a} nach (4) kongruent sein und daher der Gleichung genügen

$$\left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right) = +1,$$

d. h. der Gleichung

$$\left(\frac{\nu}{\mu}\right) = \left(\frac{\mu}{\nu}\right),$$

was übereinstimmt mit dem Gauß'schen Satze, welcher lautet:

„Bezeichnen $a+bi$, $A+Bi$ Primzahlen von der Beschaffenheit, dass a, A ungerade, b, B gerade sind, so wird entweder jede der beiden quadratischer Rest oder jede der beiden quadratischer Nichtrest der anderen sein“.

§ 8.

Zweite Bestätigung in $k\left(e^{\frac{2i\pi}{8}}\right)$.

Der Kreiskörper der 8ten Einheitswurzeln wird definirt durch die Wurzeln der Gleichung

$$x^4 + 1 = 0.$$

Bezeichnet man die Wurzel $\sqrt{i}$ mit ϱ, so sind die anderen Wurzeln ϱ^3, ϱ^5, ϱ^7. Wir geben nun die quadratischen Unterkörper von $k(\varrho)$ an, indem wir jedem die Form derjenigen rationalen Primzahlen beischreiben, welche in ihm in Primzahlen des Körpers $k(\varrho)$ zerlegt werden.

$$k(\varrho^2) = k(\sqrt{-1}): \qquad p = 8m+5.$$
$$k(\varrho - \varrho^{-1}) = k(\sqrt{-2}): p = 8m+3.$$
$$k(\varrho + \varrho^{-1}) = k(\sqrt{2}): p = 8m+7.$$

Die rationalen Primzahlen $p = 8m+1$ werden in Primzahlen ersten Grades des Körpers $k(\varrho)$ zerlegt.

Die reelle Einheit $-1+\varrho+\varrho^{-1} = -1+\sqrt{2}$, die mit ε bezeichnet werde, ist im Körper $k(\varrho)$ eine Grundeinheit, wie sich aus der Theorie der Pell'schen Gleichung beweisen lässt. Jede Einheit η von $k(\varrho)$ ist darstellbar in der Form

$$\eta = \sqrt{i}^{\,n_0} \cdot \varepsilon^{n_1},$$

wo n_0, n_1 ganzzahlige positive oder negative Exponenten bezeichnen.

Bevor wir zur Bestätigung des ersten Ergänzungsgesetzes schreiten, bestimmen wir die Relativnormen der Einheitswurzel $\sqrt{i}$ und der Einheit ε in Bezug auf die vorhandenen Unterkörper.

Die Relativnorm von $-1+\varrho+\varrho^{-1} = -1+\varrho-\varrho^3$ ist in Bezug auf den Unterkörper $k(\sqrt{-1})$

$$N_{k(\sqrt{-1})}(-1+\varrho-\varrho^3) = (-1+\varrho-\varrho^3)(-1+\varrho^p-\varrho^{3p}),$$

wo $p = 8m+5$, d. h. es ist

$$N_{k(\sqrt{-1})}(\varepsilon) = (-1+\sqrt{2})(-1-\sqrt{2}) = -1.$$

Ferner ist

$$N_{k(\sqrt{-1})}(\varepsilon) = -1,$$
$$N_{k(\sqrt{-1})}(\varepsilon) = \varepsilon^2.$$

Die Relativnormen von $\sqrt{i}$ in Bezug auf die Unterkörper $k(\sqrt{-1})$, $k(\sqrt{-2})$, $k(\sqrt{2})$ sind

$$N_{k(\sqrt{-1})}(\sqrt{i}) = \sqrt{i}\cdot\sqrt{i}^5 = -i$$
$$N_{k(\sqrt{-2})}(\sqrt{i}) = \sqrt{i}\cdot\sqrt{i}^3 = -1$$
$$N_{k(\sqrt{2})}(\sqrt{i}) = \sqrt{i}\cdot\sqrt{i}^7 = +1.$$

Bezeichnen wir jetzt die Primzahlen von $k(\varrho)$, welche in den Unterkörpern $k(\sqrt{-1})$, $k(\sqrt{-2})$, $k(\sqrt{2})$ liegen, bzw. mit $\omega_{\sqrt{-1}}$, $\omega_{\sqrt{-2}}$ $\omega_{\sqrt{2}}$, so hat man

$$\left(\frac{\sqrt{i}}{\omega_{\sqrt{-1}}}\right) \equiv (-i)^{\frac{p-1}{2}} \equiv -1, \quad (\omega_{\sqrt{-1}}),$$

$$\left(\frac{\varepsilon}{\omega_{\sqrt{-1}}}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv +1, \quad (\omega_{\sqrt{-1}}),$$

wo $p = 8m+5$.

$$\left(\frac{\sqrt{i}}{\omega_{\sqrt{-2}}}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1, \quad (\omega_{\sqrt{-2}}),$$

$$\left(\frac{\varepsilon}{\omega_{\sqrt{-2}}}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1, \quad (\omega_{\sqrt{-2}}),$$

wo $p = 8m+3$.

$$\frac{\sqrt{i}}{\omega_{\sqrt{2}}} \equiv (+1)^{\frac{p-1}{2}} \equiv +1, \quad (\omega_{\sqrt{2}}),$$

$$\frac{\varepsilon}{\omega_{\sqrt{2}}} \equiv (\varepsilon^2)^{\frac{p-1}{2}} = \varepsilon^{p-1} \equiv +1, \quad (\omega_{\sqrt{2}}),$$

wo $p = 8m+7$.

Bezeichnen wir die Primzahlen ersten Grades von $k(\sqrt{i})$ mit $\omega_{\sqrt{i}}$, so hat man zunächst

$$\left(\frac{\sqrt{i}}{\omega_{\sqrt{i}}}\right) \equiv (\sqrt{i})^{\frac{p-1}{2}}, \quad \left(\omega_{\sqrt{i}}\right),$$

wo $p = 8m+1 \begin{cases} 16m+1 \\ 16m+9. \end{cases}$

Man erhält

$$\left(\frac{\sqrt{i}}{\omega_{\sqrt{i}}}\right) = +1,$$

wenn die Norm $n\left(\omega_{\sqrt{i}}\right) = p = 16m+1$,

$$\left(\frac{\sqrt{i}}{\omega_{\sqrt{i}}}\right) = -1,$$

wenn die Norm $n\left(\omega_{\sqrt{i}}\right) = p\ 16m+9$.

Wir bestimmen jetzt den quadratischen Charakter von ε nach folgenden Primfaktoren der rationalen Primzahlen $p = 16m+1$:

$$\omega_{17}, \quad \omega_{97}, \quad \omega_{113}, \quad \omega_{193}, \quad \omega_{241}, \quad \omega_{257},$$
$$\omega_{337}, \quad \omega_{401}, \quad \omega_{433}, \quad \omega_{449}, \quad \omega_{577}, \quad \omega_{881},$$

wo der Index der Zahlen ω diejenige rationale Primzahl bezeichnet, welche durch ω teilbar ist.

Man erhält

$$\left(\frac{\varepsilon}{\omega_{17}}\right) = -1, \quad \left(\frac{\varepsilon}{\omega_{97}}\right) = -1, \quad \left(\frac{\varepsilon}{\omega_{113}}\right) = +1,$$
$$\left(\frac{\varepsilon}{\omega_{193}}\right) = -1, \quad \left(\frac{\varepsilon}{\omega_{241}}\right) = -1, \quad \left(\frac{\varepsilon}{\omega_{257}}\right) = +1,$$
$$\left(\frac{\varepsilon}{\omega_{337}}\right) = +1, \quad \left(\frac{\varepsilon}{\omega_{401}}\right) = -1, \quad \left(\frac{\varepsilon}{\omega_{433}}\right) = -1,$$
$$\left(\frac{\varepsilon}{\omega_{449}}\right) = -1, \quad \left(\frac{\varepsilon}{\omega_{577}}\right) = +1, \quad \left(\frac{\varepsilon}{\omega_{881}}\right) = +1.$$

Wir wenden uns zur Bestätigung des ersten Ergänzungsgesetzes.

Wir haben folgende primäre Hauptideale ersten Grades

$$(\omega_{113}),\quad (\omega_{257}),\quad (\omega_{337}),\quad (\omega_{577}),\quad (\omega_{881}).$$

In der That ist

$$\omega_{113} = 1-3\varrho-\varrho^3 \equiv 1+\varrho-\varrho^3,\quad (2^2),$$
$$(1-\varrho+\varrho^3)\cdot\omega_{113} \equiv i^2,\quad (2^2),$$

$$\omega_{257} = 4+\varrho \equiv \varrho,\quad (2^2),$$
$$\varrho^3\cdot\omega_{257} \equiv i^2,\quad (2^2),$$

$$\omega_{337} = 3-4\varrho \equiv i^2,\quad (2^2),$$

$$\omega_{577} = 3-\varrho+5\varrho^3 \equiv -1-\varrho+\varrho^3,\quad (2^2),$$
$$(-1+\varrho-\varrho^3)\cdot\omega_{577} \equiv i^2,\quad (2^2),$$

$$\omega_{881} = 5+4\varrho \equiv 1^2,\quad (2^2).$$

Unter den Primidealen von $k(\sqrt{i})$, welche in den Unterkörpern $k(\sqrt{-1})$, $k(\sqrt{-2})$ liegen, giebt es keine primären; dagegen sind sämmtliche Primideale von $k(\sqrt{i})$ in $k(\sqrt{2})$ primär.

Letzteres lässt sich ganz allgemein bestätigen.

Die Anzahl aller nach (2^2) inkongruenten und zu 2 primen Reste in $k(\sqrt{2})$ ist

$$\varphi(4) = n(4)\left(1-\frac{1}{n(\sqrt{2})}\right) = 8.$$

Es sind dies die folgenden Zahlen (A):

$$\text{(A)}\qquad \begin{matrix} 1+\sqrt{2}, & 1+2\sqrt{2}, & 1+3\sqrt{2}, & 1+4\sqrt{2}, \\ 3+\sqrt{2}, & 3+2\sqrt{2}, & 3+3\sqrt{2}, & 3+4\sqrt{2}. \end{matrix}$$

Nun ist jede Primzahl in $k(\sqrt{2})$ irgend einer dieser Zahlen nach (4) kongruent; denn die nach (4) inkongruenten aber zu 4 nicht primen Reste haben stets die Form

$$2n+m\sqrt{2}.$$

Wäre eine Primzahl $a+b\sqrt{2}$ einer solchen Zahl nach (4) kongruent, so müsste notwendig $a\equiv 0$, (2), also $a+b\sqrt{2}$ von der Form $2a'+b\sqrt{2}$ sein, was nicht möglich, da die Norm einer solchen

Zahl, $4a'^2 - 2b^2$, durch 2 teilbar ist. Jede Primzahl von $k(\sqrt{2})$ ist also einer der Zahlen (A) nach (4) kongruent.

Nun ist aber jeder der Reste (A) einer Einheit nach (4) kongruent. Es ist nach (4)

$$\begin{array}{ll} 1+\sqrt{2} \equiv 1+\sqrt{2} & 3+\sqrt{2} \equiv (1+\sqrt{2})^3 \\ 1+2\sqrt{2} \equiv -(1+\sqrt{2})^2 & 3+2\sqrt{2} \equiv (1+\sqrt{2})^2 \\ 1+3\sqrt{2} \equiv 1-\sqrt{2} & 3+3\sqrt{2} \equiv -(1+\sqrt{2}) \\ 1+4\sqrt{2} \equiv 1 & 3+4\sqrt{2} \equiv i^2. \end{array}$$

Also ist jede Primzahl des Körpers $k(\sqrt{2})$ einer Einheit nach (4) kongruent und daher mit einer geeigneten Einheit multiplicirt kongruent 1 nach (4).

Wir wenden uns zur Bestätigung des zweiten Ergänzungsgesetzes.

Die Zahl 2 ist in $k(\varrho)$ so zu zerlegen

$$2 = \varepsilon \cdot (1-\varrho)^4,$$

wo ε eine Einheit und $1-\varrho$ eine Primzahl ersten Grades.

Ein primäres Ideal (ω) des Körpers $k(\varrho)$ wird also dann hyperprimär sein, wenn

$$\left(\frac{1-\varrho}{\omega}\right) = +1$$

und daher

$$\varepsilon \cdot \omega \equiv \alpha^2, \quad (2^2 \cdot (1-\varrho))$$

wo ε eine Einheit und α eine ganze Zahl von $k(\varrho)$ bezeichnen.

Wir untersuchen zuerst die primären Primideale ersten Grades. Man erhält

$$\left(\frac{1-\varrho}{\omega_{113}}\right) = -1, \quad \left(\frac{1-\varrho}{\omega_{257}}\right) = -1, \quad \left(\frac{1-\varrho}{\omega_{337}}\right) = +1,$$
$$\left(\frac{1-\varrho}{\omega_{577}}\right) = +1, \quad \left(\frac{1-\varrho}{\omega_{881}}\right) = +1.$$

In Bestätigung des zweiten Ergänzungsgesetzes ist

$$\omega_{337} = 3 - 4\varrho \equiv i^2, \quad (2^2 \cdot (1-\varrho)),$$
$$\omega_{577} = 3 - \varrho + 5\varrho^2 \equiv -1 - \varrho + \varrho^2, \quad (2^2 . (1+\varrho^2)),$$

wo $1+\varrho^3 = 1-\varrho^7$ konjugirt zu $1-\varrho$ und von $1-\varrho$ um den Einheitsfaktor $\frac{1-\varrho^7}{1-\varrho}$ verschieden.

$$\omega_{8R1} = 5+4\varrho^2 \equiv 1, \quad (2^2(1+\varrho^3)).$$

Jetzt bestimmen wir unter den sämmtlich primären Primidealen des Körpers $k(\sqrt{2})$ die hyperprimären.

Man hat zunächst, indem man einen andern Primfaktor von 2, nämlich $1-\varrho^5 = 1+\varrho$ für $1-\varrho$ setzt, den Ansatz

$$\left(\frac{1+\varrho}{\omega_{\sqrt{2}}}\right) \equiv \left(N_{k\sqrt{2}}(1+\varrho)\right)^{\frac{p-1}{2}}, \quad (\omega_{\sqrt{2}}),$$

oder, da $N_{k\sqrt{2}}(1+\varrho) = (1+\varrho)(1+\varrho^7) = 2+\sqrt{2}$,

$$\left(\frac{1+\varrho}{\omega_{\sqrt{2}}}\right) \equiv (2+\sqrt{2})^{\frac{p-1}{2}}, \quad (\omega_{\sqrt{2}}).$$

Nun ist aber

$$(2+\sqrt{2})^{\frac{p-1}{2}} = \sqrt{2+\sqrt{2}}^{\,p-1} = +1, \text{ für } p = 16m+15,$$

$$\sqrt{2+\sqrt{2}}^{\,p-1} = -1, \text{ für } p = 16m+7;$$

denn $\sqrt{2+\sqrt{2}} = \sqrt[4]{i} + \sqrt[4]{i}^{-1}$ bestimmt den reellen Unterkörper des Körpers $k(\sqrt[4]{i})$. In dem reellen Körper $k\left(\sqrt{2+\sqrt{2}}\right)$ werden aber die rationalen Primzahlen $p = 16m+15$ in Primideale von $k(\sqrt[4]{i})$ zerlegt; daher ist

$$\sqrt{2+\sqrt{2}}^{\,p-1} \equiv +1 \quad (p)$$

für $p = 16m+15$; da ferner die rationalen Primzahlen $p = 16m+7$ in dem Unterkörper $k(\sqrt[4]{i} - \sqrt[4]{i}^{-1})$ in Primideale von $k(\sqrt[4]{i})$ zerlegt werden, so ist

$$\sqrt{2+\sqrt{2}}^{\,p-1} \equiv -1 \quad (p).$$

Man hat also das Resultat, dass

$$\left(\frac{1+\varrho}{\omega_{\sqrt{2}}}\right) = +1,$$

wenn $\omega_{\sqrt{2}}$ Primteiler einer rationalen Prim-Zahl $p = 16m + 15$ ist,

$$\left(\frac{1+\varrho}{\omega_{\sqrt{2}}}\right) = -1,$$

wenn $\omega_{\sqrt{2}}$ Primteiler einer rationalen Primzahl $p = 16m + 7$ ist.

Auch dieses lässt sich allgemein bestätigen.

Wir zeigen, dass jede Primzahl von $k(\varrho)$, welche Primfaktor einer rationalen Primzahl $p = 16m + 15$ ist und daher in $k(\sqrt{2})$ liegt, kongruent einer Einheit nach $(4\sqrt{2})$, und daher auch kongruent einer Einheit nach $(2^2(1+\varrho))$ ist, da

$$\sqrt{2} = (-1+\sqrt{2})\left(\frac{1+\varrho^7}{1+\varrho}\right)\cdot(1+\varrho)^2$$

und mithin folgende Hauptideale einander gleich sind

$$(4\sqrt{2}) = (4\cdot(1+\varrho)^2).$$

Die nach $(4\sqrt{2})$ inkongruenten und zu 2 primen Reste des Körpers $k(\sqrt{2})$ sind folgende:

$$\left.\begin{matrix} 1+\sqrt{2}, & 1+2\sqrt{2}, & 1+3\sqrt{2}, & 1+4\sqrt{2}, \\ 3+\sqrt{2}, & 3+2\sqrt{2}, & 3+3\sqrt{2}, & 3+4\sqrt{2}, \\ 5+\sqrt{2}, & 5+2\sqrt{2}, & 5+3\sqrt{2}, & 5+4\sqrt{2}, \\ 7+\sqrt{2}, & 7+2\sqrt{2}, & 7+3\sqrt{2}, & 7+4\sqrt{2}. \end{matrix}\right\} \quad (B.)$$

Da nun jede Primzahl des Körpers $k(\sqrt{2})$ irgend einem der Reste (B) nach $(4\sqrt{2})$ kongruent ist, so suchen wir unter den Resten (B) diejenigen aus, welche einer Einheit kongruent nach $(4\sqrt{2})$ ausfallen.

Nun giebt es nach $(4\sqrt{2})$ vier verschiedene Potenzen von $1+\sqrt{2}$ oder von $1-\sqrt{2}$; man findet, dass nach $(4\sqrt{2})$

$$\left.\begin{array}{ll}(1+\sqrt{2})^1 \equiv 1+\sqrt{2} & (1-\sqrt{2})^1 \equiv 1-\sqrt{2} \\ (1+\sqrt{2})^2 \equiv 3+2\sqrt{2} & (1-\sqrt{2})^2 \equiv 3-2\sqrt{2} \\ (1+\sqrt{2})^3 \equiv 7+\sqrt{2} & (1-\sqrt{2})^3 \equiv 7-\sqrt{2} \\ (1+\sqrt{2})^4 \equiv 1 & (1-\sqrt{2})^4 \equiv 1\end{array}\right\}, (4\sqrt{2})$$

Unter den Resten (B) sind es also die folgenden 8, welche einer Einheit nach $(4\sqrt{2})$ kongruent sind

$$\begin{array}{lll} 1+\sqrt{2}, & 1+3\sqrt{2}, & 1+4\sqrt{2} \\ 3+2\sqrt{2}, & 5+2\sqrt{2} & \\ 7+\sqrt{2}, & 7+3\sqrt{2}, & 7+4\sqrt{2}. \end{array}$$

Wenn aber eine Zahl in $k(\sqrt{2})$ einer dieser 8 Zahlen nach $(4\sqrt{2})$ kongruent ist, so besitzt sie notwendig eine der folgenden beiden Formen

$$\begin{array}{ll} \text{I.} & (8m \pm 1) \pm (4n \pm 1)\sqrt{2} \\ \text{II.} & (8m \pm 3) \pm (4n \pm 2)\sqrt{2}. \end{array}$$

Hat eine Primzahl in $k(\sqrt{2})$ die Form I, so ist ihre Norm in $k(\sqrt{2})$ von der Form $16m+5$, und umgekehrt, hat eine Primzahl in $k(\sqrt{2})$ eine Norm von der Form $16m+5$, so ist sie selbst von der Form I und daher einer Einheit kongruent nach $(4\sqrt{2})$.

Hat eine Primzahl in $k(\sqrt{2})$ die Form II, so ist ihre Norm in $k(\sqrt{2})$ von der Form $16m+1$ und ist daher keine Primzahl in $k(\varrho)$, sondern eine Zahl in $k(\sqrt{2})$, welche in $k(\varrho)$ in zwei Primzahlen ersten Grades zerlegt wird.

Wir wenden uns zur Bestätigung des Korollares des Satzes 3 im Körper $k(\varrho)$. Darnach ist, wenn ν, μ ganze Zahlen in $k(\varrho)$ sind, von denen mindestens eine primär ist,

$$\left(\frac{\nu}{\mu}\right) = \left(\frac{\mu}{\nu}\right).$$

Sei $\omega_{\sqrt{2}}$ irgend eine in $k(\sqrt{2})$ gelegene primäre Primzahl des Körpers $k(\varrho)$, und seien $\omega_{\sqrt{-2}}, \omega_{\sqrt{-1}}$, irgend welche in $k\sqrt{-2}$, $k\sqrt{-1}$ gelegene Primzahlen von $k(\varrho)$. Wir bestätigen dann folgende

zwei Gleichungen

$$\text{I.}\quad \left(\frac{\omega_{\sqrt{2}}}{\omega_{\sqrt{-2}}}\right) = \left(\frac{\omega_{\sqrt{-2}}}{\omega_{\sqrt{2}}}\right)$$

$$\text{II.}\quad \left(\frac{\omega_{\sqrt{2}}}{\omega_{\sqrt{-1}}}\right) = \left(\frac{\omega_{\sqrt{-1}}}{\omega_{\sqrt{2}}}\right).$$

Der Beweis dieser Gleichungen lässt sich sehr kurz und bündig geben, nachdem folgende Thatsache festgestellt ist.

Die Norm einer jeden primären Primzahl $\omega_{\sqrt{2}}$ in $k(\sqrt{2})$ ist negativ, d. h. es ist

$$n(\omega_{\sqrt{2}}) = -q,$$

wo q eine rationale Primzahl von der Form $4n+3$ ist. In der That, da jede Primzahl in $k(\sqrt{2})$ irgend einer der Einheiten

$$\pm(1+\sqrt{2})^1,\quad \pm(1+\sqrt{2})^2,\quad \pm(1+\sqrt{2})^3,\quad \pm(1+\sqrt{2})^4$$

nach (4) kongruent ist, so ist jede primäre Primzahl $\omega_{\sqrt{2}}$ irgend einem der vier inkongruenten Einheitsquadrate

$$1^2,\quad i^2,\quad (1+\sqrt{2})^2,\quad i^2\cdot(1+\sqrt{2})^2$$

nach 4 kongruent. Nun ist

$$\left.\begin{aligned} 1+2\sqrt{2} &\equiv i^2(1+\sqrt{2})^2, & 3+2\sqrt{2} &\equiv (1+\sqrt{2})^2 \\ 1+4\sqrt{2} &\equiv 1^2, & 3+4\sqrt{2} &\equiv i^2 \end{aligned}\right\},\quad (4)$$

wo also $1+2\sqrt{2}$, $3+2\sqrt{2}$, $1+4\sqrt{2}$, $3+4\sqrt{2}$ einander nach (4) inkongruente Reste sind.

Hieraus folgt, dass jede primäre Primzahl $\omega_{\sqrt{2}}$ von einer der folgenden beiden Formen ist

$$\text{I.}\quad (4n\pm1)\pm(4m\pm2)\sqrt{2}$$

$$\text{II.}\quad (4n\pm1)\pm(4m\pm4)\sqrt{2}.$$

Die Norm jeder Primzahl von einer dieser Formen ist aber kongruent 1 nach (4) und da $\omega_{\sqrt{2}}$ eine solche Form besitzt, so

muss die Norm

$$n(\omega_{\sqrt{2}}) \equiv 1, \quad (4)$$

in $k(\sqrt{2})$ sein; da andrerseits $n(\omega_{\sqrt{2}})$ gleich $+q$ oder gleich $-q$, wo q von der Form $4n+3$, so ist gewiss

$$n(\omega_{\sqrt{2}}) = -q.$$

Die Richtigkeit der Gleichungen I, II beweisen wir jetzt, wie folgt.

Es ist

$$\left(\frac{\omega_{\sqrt{2}}}{\omega_{\sqrt{-2}}}\right) = \left(N_{k\sqrt{-2}}(\omega_{\sqrt{2}})\right)^{\frac{q'-1}{2}}, \quad (\omega_{\sqrt{-2}}),$$

wo q' gleich der Norm von $\omega_{\sqrt{-2}}$ in $k(\sqrt{-2})$ ist; dieselbe ist immer eine positive rationale Primzahl von der Form $4n+3$. Da nun die Relativnorm $N_{k\sqrt{-2}}(\omega_{\sqrt{2}})$ offenbar gleich der Norm von $\omega_{\sqrt{2}}$ in $k(\sqrt{2})$, d. h. gleich $-q$ ist, so schreiben wir

$$\left(\frac{\omega_{\sqrt{2}}}{\omega_{\sqrt{-2}}}\right) \equiv (-q)^{\frac{q'-1}{2}}, \quad (q').$$

Ferner ist

$$\left(\frac{\omega_{\sqrt{-2}}}{\omega_{\sqrt{2}}}\right) \equiv \left(N_{k\sqrt{2}}(\omega_{\sqrt{-2}})\right)^{\frac{q-1}{2}}, \quad (\omega_{\sqrt{2}});$$

da aber wiederum $N_{k\sqrt{2}}(\omega_{\sqrt{-2}})$ nichts anderes als die Norm von $\omega_{\sqrt{-2}}$ in $k(\sqrt{-2})$, d. h. gleich q' ist, so hat man

$$\left(\frac{\omega_{\sqrt{-2}}}{\omega_{\sqrt{2}}}\right) \equiv (q')^{\frac{q-1}{2}} \quad (q).$$

Nun ist aber

$$(-q)^{\frac{q'-1}{2}} \equiv \left(\frac{-q}{q'}\right), \quad (q')$$

$$(q')^{\frac{q-1}{2}} \equiv \left(\frac{q'}{q}\right), \quad (q),$$

also nach dem quadratischen Reciprocitätsgesetz der rationalen Primzahlen

$$\left(\frac{-q}{q'}\right) = \left(\frac{q'}{q}\right),$$

und folglich

$$\left(\frac{\omega_{\sqrt{2}}}{\omega_{\sqrt{-2}}}\right) = \left(\frac{\omega_{\sqrt{-2}}}{\omega_{\sqrt{2}}}\right),$$

womit die Gleichung I bewiesen ist.

In ganz entsprechender Weise beweisen wir die Gleichung II:

$$\left(\frac{\omega_{\sqrt{2}}}{\omega_{\sqrt{-1}}}\right) = \left(\frac{\omega_{\sqrt{-1}}}{\omega_{\sqrt{2}}}\right).$$

Da wieder die Relativnorm $N_{k(\sqrt{-1})}(\omega_{\sqrt{2}})$ gleich der Norm von $\omega_{\sqrt{2}}$ in $k(\sqrt{2})$ und die Relativnorm $N_{k(\sqrt{2})}(\omega_{\sqrt{-1}})$ gleich der Norm von $\omega_{\sqrt{-1}}$ in $k(\sqrt{-1})$, d. h. gleich einer positiven rationalen Primzahl $p = 4n+1$ ist, so hat man

$$\left(\frac{\omega_{\sqrt{2}}}{\omega_{\sqrt{-1}}}\right) \equiv \left(N_{k(\sqrt{-1})}(\omega_{\sqrt{2}})\right)^{\frac{p-1}{2}} \equiv \left(n(\omega_{\sqrt{2}})\right)^{\frac{p-1}{2}} \equiv (-q)^{\frac{p-1}{2}}, \quad (\omega_{\sqrt{-1}})$$

$$\left(\frac{\omega_{\sqrt{-1}}}{\omega_{\sqrt{2}}}\right) \equiv \left(N_{k(\sqrt{2})}(\omega_{\sqrt{-1}})\right)^{\frac{q-1}{2}} \equiv \left(n(\omega_{\sqrt{-1}})\right)^{\frac{q-1}{2}} \equiv (p)^{\frac{q-1}{2}}, \quad (\omega_{\sqrt{2}}).$$

Also, da

$$(-q)^{\frac{p-1}{2}} \equiv \left(\frac{-q}{p}\right), \quad (p)$$

$$(p)^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right), \quad (q)$$

und

$$\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right),$$

so folgt

$$\left(\frac{\omega_{\sqrt{2}}}{\omega_{\sqrt{-1}}}\right) = \left(\frac{\omega_{\sqrt{-1}}}{\omega_{\sqrt{2}}}\right),$$

welches die Gleichung II ist.

§ 9.

Dritte Bestätigung in $k\left(e^{\frac{2i\pi}{16}}\right)$.

Der Kreiskörper der 16ten Einheitswurzeln wird definirt durch die Wurzeln der Gleichung

$$x^8 + 1 = 0 \quad \text{I.}$$

Indem wir mit θ eine bestimmte Wurzel der Gleichung I, bezeichnen, nennen wir den Zahlkörper $K(\theta)$. Derselbe besitzt die Klassenanzahl 1.

Die bestimmenden Zahlen der biquadratischen Unterkörper sind

$$\theta^2 = \varrho, \quad \theta + \theta^{-1} = \vartheta, \quad \theta - \theta^{-1} = \eta.$$

Die bestimmenden Zahlen der quadratischen Unterkörper sind

$$\theta^4 = \sqrt{-1}, \quad \theta^2 + \theta^{-2} = \sqrt{2}, \quad \theta^2 - \theta^{-2} = \sqrt{-2}.$$

Indem wir jetzt mit

p_1	die rationalen Primzahlen	der Form	$16m+1$
p_3	"	"	$16m+3$
p_5	"	"	$16m+5$
p_7	"	"	$16m+7$
p_9	"	"	$16m+9$
p_{11}	"	"	$16m+11$
p_{13}	"	"	$16m+13$
p_{15}	"	"	$16m+15$

bezeichnen, sprechen wir auf Grund der Sätze des § 3 folgende Thatsachen aus.

1) Die rationalen Primzahlen von der Form $16m+1$ werden in Primideale ersten Grades von $K(\theta)$ zerlegt. Die Substitution $\sigma = (\theta : \theta^{p_1})$ ist die identische, sie lässt alle Zahlen des Körpers $K(\theta)$ ungeändert.

2) Die rationalen Primzahlen $p_{15} = 16m+15$ werden in Primideale zweiten Grades von $K(\theta)$ zerlegt, welche vom ersten Grade im Unterkörper $k(\theta+\theta^{-1}) = k(\vartheta)$ sind. Die Substitutionen $\sigma = (\theta : \theta^{p_{15}})$, $\sigma_2 = (\theta : \theta^{p_{15}^2}) = 1$, d. h. $\sigma = (\theta : \theta^{15})$, $\sigma^2 = (\theta : \theta^{15^2}) = 1$ bilden die zu $k(\vartheta)$ gehörende Untergruppe.

3) Die rationalen Primzahlen $p_7 = 16m+7$ werden in Primideale zweiten Grades von $K(\theta)$ zerlegt, welche vom ersten Grade im Unterkörper $k(\theta-\theta^{-1}) = k(\eta)$ sind. Die Substitutionen $\sigma = (\theta:\theta^{p_7})$, $\sigma^2 = (\theta:\theta^{p_7^2}) = 1$, d. h. $\sigma = (\theta:\theta^7)$, $\sigma^2 = (\theta:\theta^{7^2}) = 1$ bilden die zu $k(\eta)$ gehörende Untergruppe.

4) Die rationalen Primzahlen $p_9 = 16m+9$ werden in Primideale zweiten Grades von $K(\theta)$ zerlegt, welche vom ersten Grade im Unterkörper $k(\varrho)$ sind. Die Substitutionen $\sigma = (\theta:\theta^{p_9})$, $\sigma^2 = (\theta:\theta^{p_9^2}) = 1$, d. h. $\sigma = (\theta:\theta^9)$, $\sigma^2 = (\theta:\theta^{81}) = 1$ bilden, die zu $k(\varrho)$ gehörende Untergruppe.

5) Die rationalen Primzahlen von der Form $8m+5 = \begin{cases}16m'+5\\16m'+13\end{cases}$ werden in Primideale vierten Grades von $K(\theta)$ zerlegt, welche vom ersten Grade in dem quadratischen Unterkörper $k(\theta^4) = k(\sqrt{-1})$ sind. Die Substitutionen $\sigma = (\theta:\theta^{p_5})$, $\sigma^2 = (\theta:\theta^{p_5^2})$, $\sigma^3 = (\theta:\theta^{p_5^3})$, $\sigma^4 = (\theta:\theta^{p_5^4}) = 1$, oder $\sigma' = (\theta:\theta^{p_{13}})$, $\sigma'^2 = (\theta:\theta^{p_{13}^2})$, $\sigma'^3 = (\theta:\theta^{p_{13}^3})$, $\sigma'^4 = (\theta:\theta^{p_{13}^4}) = 1$, d. h. $\sigma = (\theta:\theta^5)$, $\sigma^2 = (\theta:\theta^9)$, $\sigma^3 = (\theta:\theta^{13})$, $\sigma^4 = (\theta:\theta^1) = 1$ bilden die zu $k(\sqrt{-1})$ gehörende Untergruppe.

6) Die rationalen Primzahlen von der Form $8m+3 = \begin{cases}16m'+3\\16m'+11\end{cases}$ werden in Primideaie vierten Grades von $K(\theta)$ zerlegt, welche vom ersten Grade in dem quadratischen Unterkörper $k(\sqrt{-2})$ sind. Die Substitutionen $\sigma = (\theta:\theta^{p_3})$, $\sigma^2 = (\theta:\theta^{p_3^2})$, $\sigma^3 = (\theta:\theta^{p_3^3})$, $\sigma^4 = (\theta:\theta^{p_3^4}) = 1$, oder $\sigma' = (\theta:\theta^{p_{11}})$, $\sigma'^2 = (\theta:\theta^{p_{11}^2})$, $\sigma'^3 = (\theta:\theta^{p_{11}^3})$, $\sigma'^4 = (\theta:\theta^{p_{11}^4}) = 1$, d. h. $\sigma = (\theta:\theta^3)$, $\sigma^2 = (\theta:\theta^9)$, $\sigma^3 = (\theta:\theta^{11})$, $\sigma^4 = (\theta:\theta^1) = 1$, oder $\sigma' = (\theta:\theta^{11})$, $\sigma'^2 = (\theta:\theta^9)$, $\sigma'^3 = (\theta:\theta^3)$, $\sigma'^4 = (\theta:\theta^1) = 1$ bilden die zu $k(\sqrt{-2})$ gehörende Untergruppe.

Hierzu ist noch zu bemerken, dass in den Unterkörpern $k(\sqrt{2})$ und $k(1)$ gemäss § 3 keine Primideale von $K(\theta)$ liegen.

Was die Einheiten anbetrifft, so liegt das in § 5 charakterisirte System konjugirter Einheiten in dem reellen cyklischen Unterkörper $k(\theta+\theta^{-1}) = k(\vartheta)$ zugrunde. Wir bestimmen zunächst die Gleichung, welche diesen Körper definirt.

Vermöge

$$\theta^8+1 = 0$$

ist

$$\theta^4+\theta^{-4} = 0.$$

Ferner ist

$$\vartheta^4 = (\theta + \theta^{-1})^4 = \theta^4 + 4\theta^2 + 6 + 4\theta^{-2} + \theta^{-4}$$
$$= 4(\theta^2 + \theta^{-2}) + 6.$$

Da nun $(\theta + \theta^{-1})^2 = \theta^2 + \theta^{-2} + 2$, so ist

$$\vartheta^4 - 4\vartheta^2 + 2 = 0. \quad \text{II.}$$

Sind die vier Wurzeln dieser Gleichung ϑ, ϑ', ϑ'', ϑ''', so hat man

$$\begin{aligned} \vartheta &= \theta + \theta^{-1} = \theta - \theta^7 \\ \vartheta' &= -\theta - \theta^{-1} = -\theta + \theta^7 \\ \vartheta'' &= \theta^3 + \theta^{-3} = \theta^3 - \theta^5 \\ \vartheta''' &= -\theta^3 - \theta^{-3} = -\theta^3 + \theta^5. \end{aligned}$$

Im Besonderen ist noch

$$\vartheta = \sqrt{2+\sqrt{2}}, \quad \vartheta' = -\sqrt{2+\sqrt{2}}$$
$$\vartheta'' = \sqrt{2-\sqrt{2}}, \quad \vartheta''' = -\sqrt{2-\sqrt{2}}.$$

Wir schreiben jetzt die Identität in x:

$$x^4 - 4x^2 + 2 = (x - \vartheta)(x - \vartheta')(x - \vartheta'')(x - \vartheta''').$$

Für $x = 1$ hat man also

$$(1 - \vartheta)(1 - \vartheta')(1 - \vartheta'')(1 - \vartheta''') = -1.$$

Die 4 Faktoren auf der linken Seite der Gleichung sind das System konjugirter Einheiten, von denen irgend welche drei nebst der Einheitswurzel θ, zur Bestätigung des Reciprocitätsgesetzes zu verwenden sind. Den Beweis hierfür erbringen wir weiter unten.

Wir führen folgende Bezeichnungen ein:

$$\begin{aligned} \varepsilon_1 &= 1 - \vartheta = 1 - \theta + \theta^7 \\ \varepsilon_2 &= 1 - \vartheta' = 1 + \theta - \theta^7 \\ \varepsilon_3 &= 1 - \vartheta'' = 1 - \theta^3 + \theta^5 \\ \varepsilon_4 &= 1 - \vartheta''' = 1 + \theta^3 - \theta^5. \end{aligned}$$

Wir wollen die quadratischen Charaktere aller vier Einheiten bestimmen und zwar aus Zweckmässigkeitsgründen, obwohl belie-

bige drei dieser Einheiten nebst θ zu den Bestätigungen ausreichend sind.

Ferner soll unter konjugirten Primidealen nur eines zur Bestimmung des quadratischen Charakters der Einheiten nach demselben verwendet werden, da konjugirte Primideale gleichzeitig primär oder nicht primär sind. Seien nämlich $\varphi(\theta)$ und $\varphi(\theta')$ konjugirte Primzahlen von $K(\theta)$ und sei $\varphi(\theta)$ primär, so ist nach der Definition

$$\left(\frac{\theta}{\varphi(\theta)}\right) = +1, \quad \left(\frac{\varepsilon_1}{\varphi(\theta)}\right) = \left(\frac{\varepsilon_2}{\varphi(\theta)}\right) = \left(\frac{\varepsilon_3}{\varphi(\theta)}\right) = \left(\frac{\varepsilon_4}{\varphi(\theta)}\right) = +1.$$

Nun ist offenbar, wenn wir auf die Einheiten die Substitution $\sigma = (\theta : \theta')$ anwenden

$$\left(\frac{\theta'}{\varphi(\theta')}\right) = \left(\frac{\theta}{\varphi(\theta)}\right), \quad \left(\frac{\varepsilon_1(\theta')}{\varphi(\theta')}\right) = \left(\frac{\varepsilon_1(\theta)}{\varphi(\theta)}\right), \quad \left(\frac{\varepsilon_2(\theta')}{\varphi(\theta')}\right) = \left(\frac{\varepsilon_2(\theta)}{\varphi(\theta)}\right),$$
$$\left(\frac{\varepsilon_3(\theta')}{\varphi(\theta')}\right) = \left(\frac{\varepsilon_3(\theta)}{\varphi(\theta)}\right), \quad \left(\frac{\varepsilon_4(\theta')}{\varphi(\theta')}\right) = \left(\frac{\varepsilon_4(\theta)}{\varphi(\theta)}\right).$$

Da aber der Komplex der Einheiten $\varepsilon_1(\theta')$, $\varepsilon_2(\theta')$, $\varepsilon_3(\theta')$, $\varepsilon_4(\theta')$ identisch ist mit den Einheiten $\varepsilon_1(\theta)$, $\varepsilon_2(\theta)$, $\varepsilon_3(\theta)$, $\varepsilon_4(\theta)$, so folgt, dass auch $\varphi(\theta')$ eine primäre Zahl von $K(\theta)$ ist.

Da also alle konjugirten Zahlen primär sind, sobald eine derselben primär ist, so folgt, dass auch alle konjugirten Zahlen nicht primär sind, sobald eine derselben nicht primär ist.

Bezeichne nun ω_k irgend eine in der rationalen Primzahl p aufgehende Primzahl des Körpers $K(\theta)$, welche in dem Unterkörper k von $K(\theta)$ liegt, so werden wir nach § 4 setzen

$$\left(\frac{\varepsilon}{\omega_k}\right) \equiv \left(N_k(\varepsilon)\right)^{\frac{p-1}{2}}, \quad (\omega_k),$$

wo $N_k(\varepsilon)$ die Relativnorm der Einheit ε in Bezug auf den Unterkörper k bezeichnet. Man hat also

$$N_k(\varepsilon) = \varepsilon(\theta) \cdot \varepsilon(\theta)^p$$

beziehungsweise

$$N_k(\varepsilon) = \varepsilon(\theta) \cdot \varepsilon(\theta^p) \cdot \varepsilon(\theta^{p^2}) \cdot \varepsilon(\theta^{p^3}),$$

je nachdem der Unterkörper k vom vierten Grade (erste Glei-

chung) oder vom zweiten Grade (zweite Gleichung) ist, d. h. je nachdem die Untergruppe, die zu k gehört, durch

$$\sigma = (\theta : \theta^p), \quad \sigma^2 = (\theta : \theta^{p^2}) = 1$$

oder durch

$$\sigma = (\theta : \theta^p), \quad \sigma^2 = (\theta : \theta^{p^2}), \quad \sigma^3 = (\theta : \theta^{p^3}), \quad \sigma^4 = (\theta : \theta^{p^4}) = 1$$

gegeben wird.

Hiernach ergiebt sich im Besonderen, wenn wir mit $N_{k(\varrho)}$, $N_{k(\eta)}$, $N_{k(\vartheta)}$, $N_{k(\sqrt{-1})}$, $N_{k(\sqrt{-2})}$ die Relativnormen in Bezug auf die Unterkörper $k(\varrho)$, $k(\eta)$, $k(\vartheta)$, $k(\sqrt{-1})$, $k(\sqrt{-2})$, und mit $\varepsilon_{1,2,3,4}$ beliebig jede der Einheiten ε_1, ε_2, ε_3, ε_4, mit $\varepsilon_{1,2}$ jede der Einheiten ε_1, ε_2, endlich mit $\varepsilon_{3,4}$ jede der Einheiten ε_3, ε_4 bezeichnen

$$N_{k(\varrho)}(\varepsilon_{1,2}) = N_{k(\eta)}(\varepsilon_{1,2}) = -1 - \sqrt{2}$$
$$N_{k(\varrho)}(\varepsilon_{3,4}) = N_{k(\eta)}(\varepsilon_{3,4}) = -1 + \sqrt{2}$$
$$N_{k(\vartheta)}(\varepsilon_{1,2,3,4}) = (\varepsilon_{1,2,3,4})^2,$$
$$N_{k\sqrt{-1}}(\varepsilon_{1,2,3,4}) = N_{k\sqrt{-2}}(\varepsilon_{1,2,3,4}) = -1.$$

Ferner ist:

$$N_{k(\varrho)}(\theta) = -\varrho, \quad N_{k(\eta)}(\theta) = -1,$$
$$N_{k(\vartheta)}(\theta) = +1.$$
$$N_{k\sqrt{-1}}(\theta) = -i, \quad N_{k(\sqrt{-2})}(\theta) = -1.$$

Wir bezeichnen jetzt mit ω_ϱ, ω_η, ω_ϑ, $\omega_{\sqrt{-1}}$, $\omega_{\sqrt{-2}}$ Primzahlen des Körpers $K(\theta)$, welche bezüglich in den Unterkörpern $k(\varrho)$, $k(\eta)$, $k(\vartheta)$, $k(\sqrt{-1})$, $k(\sqrt{-2})$ liegen; mit ω_θ sollen Primzahlen ersten Grades von $K(\theta)$ bezeichnet sein.

Was zunächst die Primzahlen $\omega_{\sqrt{-1}}$, $\omega_{\sqrt{-2}}$, ω_ϑ angeht, so können wir nach diesen sämmtlichen Primzahlen mit Leichtigkeit die quadratischen Charaktere der Einheiten berechnen.

1) Für die Primfaktoren $\omega_{\sqrt{-1}}$ der rationalen Primzahlen

$$p \overset{\shortmid}{=} \begin{Bmatrix} 16m+5 \\ 16m+13 \end{Bmatrix} = 8m'+5$$

hat man

$$\left(\frac{\varepsilon_{1,2,3,4}}{\omega_{\sqrt{-1}}}\right) \equiv (-1)^{\frac{p-1}{2}}, \quad \left(\omega_{\sqrt{-1}}\right),$$

d. h. da $\dfrac{8m'+5-1}{2} = 2(2m'+1)$,

$$\left(\frac{\varepsilon_{1,2,3,4}}{\omega_{\sqrt{-1}}}\right) = +1;$$

ferner ist

$$\left(\frac{\theta}{\omega_{\sqrt{-1}}}\right) \equiv (-i)^{\frac{p-1}{2}} \equiv -1, \quad \left(\omega_{\sqrt{-1}}\right).$$

2) Die rationalen Primzahlen p, deren Primfaktoren in $k(\sqrt{-2})$ liegen, haben die Form

$$p = 8m+3 = \begin{cases} 16m'+3 \\ 16m'+11. \end{cases}$$

Also ist

$$\left(\frac{\varepsilon_{1,2,3,4}}{\omega_{\sqrt{-2}}}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1, \quad \left(\omega_{\sqrt{-2}}\right),$$

$$\left(\frac{\theta}{\omega_{\sqrt{-2}}}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1, \quad \left(\omega_{\sqrt{-2}}\right),$$

3) Die rationalen Primzahlen, deren Primfaktoren in $k(\vartheta)$ liegen, haben die Form

$$p = 16m+15.$$

Daher ist

$$\left(\frac{\theta}{\omega_{\vartheta}}\right) \equiv (+1)^{\frac{p-1}{2}} \equiv +1, \quad \left(\omega_{\vartheta}\right),$$

$$\left(\frac{\varepsilon_{1,2,3,4}}{\omega_{\vartheta}}\right) \equiv \left\{(\varepsilon_{1,2,3,4})^2\right\}^{\frac{p-1}{2}} \equiv +1, \quad \left(\omega_{\vartheta}\right),$$

denn, da $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ Zahlen in $k(\vartheta)$ sind, so ist nach dem Fermat'schen Satze

$$(\varepsilon_{1,2,3,4})^{n(\omega_{\vartheta})-1} \equiv +1, \quad \left(\omega_{\vartheta}\right),$$

wo $n\left(\omega_{\vartheta}\right)$ die Norm von ω_{ϑ} in $k(\vartheta)$ bezeichnet. Es ist aber

$$n\left(\omega_{\vartheta}\right) = p^2.$$

Was die in $k(\varrho)$ und $k(\eta)$ liegenden Primzahlen ω_ϱ, ω_η anbetrifft, sowie die Primzahlen ersten Grades ω_θ, so lassen sich die quadratischen Charaktere der Einheiten ε nach denselben nur im einzelnen Falle, nicht allgemein, wenigstens nach den entwickelten Methoden, bestimmen, doch sind gewiss alle Primzahlen ω_ϱ und ω_η nichtprimär, da

$$\left(\frac{\theta}{\omega_\varrho}\right) \equiv (-\varrho)^{\frac{p-1}{2}} \equiv -1, \quad (\omega_\varrho)$$
$$\left(\frac{\theta}{\omega_\eta}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1, \quad (\omega_\eta)$$

ausfällt.

Nach denjenigen Primzahlen ersten Grades ferner, welche in den rationalen Primzahlen

$$p = 32m+1$$

aufgehen, ist

$$\left(\frac{\theta}{\omega_\theta}\right) \equiv \theta^{\frac{p-1}{2}} \equiv +1, \quad (\omega_\theta).$$

Geht aber ω_θ in einer rationalen Primzahl

$$p = 16m+1 = 32m+17$$

auf, so wird

$$\left(\frac{\theta}{\omega_\theta}\right) \equiv \theta^{\frac{p-1}{2}} \equiv -1, \quad (\omega_\theta).$$

Es mögen also:

4) Folgende Primzahlen ω_ϱ zur Berechnung verwendet werden:

$$\omega_{41}, \ \omega_{73}, \ \omega_{89}, \ \omega_{137}, \ \omega_{233}, \ \omega_{281},$$

wo die ω beigeschriebene rationale Primzahl diejenige ist, in welcher die betreffende Primzahl ω von $K(\theta)$ aufgeht.

Zuvor noch eine allgemeine Bemerkung. Es ist

$$\left(\frac{\varepsilon_{1,2}}{\omega_\varrho}\right) \equiv (-1-\sqrt{2})^{\frac{p-1}{2}}, \quad (\omega_\varrho)$$
$$\left(\frac{\varepsilon_{3,4}}{\omega_\varrho}\right) \equiv (-1+\sqrt{2})^{\frac{p-1}{2}}, \quad (\omega_\varrho).$$

Aus $\left(\frac{\varepsilon_{1,2}}{\omega_\varrho}\right)$ folgt aber $\left(\frac{\varepsilon_{3,4}}{\omega_\varrho}\right)$ denn

$$\left(\frac{\varepsilon_{1,2}}{\omega_\varrho}\right)\cdot\left(\frac{\varepsilon_{3,4}}{\omega_\varrho}\right) = \left(\frac{-1}{\omega_\varrho}\right) = +1,$$

d. h.

$$\left(\frac{\varepsilon_{1,2}}{\omega_\varrho}\right) = \left(\frac{\varepsilon_{3,4}}{\omega_\varrho}\right).$$

Wir wenden uns zur Berechnung. Es ist

$$\sqrt{2} = \varrho - \varrho^3,$$

also

$$-1-\sqrt{2} = -1-\varrho+\varrho^3$$
$$-1+\sqrt{2} = -1+\varrho-\varrho^3.$$

Indem wir aus den Tafeln von Reuschle für ϱ die nach ω_ϱ kongruenten rationalen Zahlen setzen, erhalten wir:

$$\begin{aligned}
-1-\sqrt{2} = -1-\varrho+\varrho^3 &\equiv 16, \quad (41),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 40, \quad (73),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 63, \quad (89),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 30, \quad (137),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 84, \quad (233),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 148, \; (281).
\end{aligned}$$

Aus den Tafeln des canon arithmeticus ferner entnimmt man:

$$A \left\{\begin{array}{llll}
\text{ind } 16 = 24 & \text{mod } 41\\
\text{ind } 40 = 25 & \text{mod } 73\\
\text{ind } 63 = 5 & \text{mod } 89\\
\text{ind } 30 = 30 & \text{mod } 137\\
\text{ind } 84 = 27 & \text{mod } 233\\
\text{ind } 148 = 253 & \text{mod } 281.
\end{array}\right.$$

Ferner ist

$$\begin{aligned}
-1+\sqrt{2} = -1+\varrho-\varrho^3 &\equiv 23, \quad (41),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 31, \quad (71),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 24, \quad (89),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 105, \; (137),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 147, \; (233),\\
\text{„} \qquad\quad \text{„} \qquad &\equiv 131, \; (281)
\end{aligned}$$

und

$$B\left\{\begin{array}{l} \text{ind } 23 = 36 \text{ mod } 41 \\ \text{ind } 31 = 11 \text{ mod } 73 \\ \text{ind } 24 = 39 \text{ mod } 89 \\ \text{ind } 105 = 38 \text{ mod } 127 \\ \text{ind } 147 = 89 \text{ mod } 233 \\ \text{ind } 131 = 167 \text{ mod } 281. \end{array}\right.$$

In Bestätigung obiger allgemeinen Bemerkung findet sich, dass die zu gleichen Moduln gehörenden Indices der Reihen A und B beide gerade oder beide ungerade sind.

Hiernach erhält man

$$\left(\frac{\varepsilon_{1,2}}{\omega_{41}}\right) = \left(\frac{\varepsilon_{3,4}}{\omega_{41}}\right) = +1,$$
$$\left(\frac{\varepsilon_{1,2}}{\omega_{73}}\right) = \left(\frac{\varepsilon_{3,4}}{\omega_{73}}\right) = -1,$$
$$\left(\frac{\varepsilon_{1,2}}{\omega_{89}}\right) = \left(\frac{\varepsilon_{3,4}}{\omega_{89}}\right) = -1,$$
$$\left(\frac{\varepsilon_{1,2}}{\omega_{137}}\right) = \left(\frac{\varepsilon_{3,4}}{\omega_{137}}\right) = +1,$$
$$\left(\frac{\varepsilon_{1,2}}{\omega_{233}}\right) = \left(\frac{\varepsilon_{3,4}}{\omega_{233}}\right) = -1,$$
$$\left(\frac{\varepsilon_{1,2}}{\omega_{251}}\right) = \left(\frac{\varepsilon_{3,4}}{\omega_{281}}\right) = -1.$$

5) Von den Primzahlen ω_η verwenden wir folgende:

$$\omega_7, \; \omega_{23}, \; \omega_{71}, \; \omega_{103}, \; \omega_{151}, \; \omega_{167}.$$

Wiederum ist allgemein zu setzen

$$\left(\frac{\varepsilon_{1,2}}{\omega_\eta}\right) = (-1-\sqrt{2})^{\frac{p-1}{2}}, \quad (\omega_\eta),$$
$$\left(\frac{\varepsilon_{3,4}}{\omega_\eta}\right) = (-1+\sqrt{2})^{\frac{p-1}{2}}, \quad (\omega_\eta).$$

Da nun

$$\left(\frac{\varepsilon_{1,2}}{\omega_\eta}\right)\left(\frac{\varepsilon_{3,4}}{\omega_\eta}\right) = \left(\frac{-1}{\omega_\eta}\right) = -1$$

ist, so wird

$$\left(\frac{s_{1,2}}{\omega_\eta}\right) = -\left(\frac{s_{3,4}}{\omega_\eta}\right).$$

Indem man nach den Tafeln von Reuschle für η die nach ω_η kongruenten rationalen Zahlen verwendet, erhält man

$$\begin{array}{lllll} -1+\sqrt{2} & = \eta^2+1 & \equiv 2, & (7), \\ \text{"} & \text{"} & \equiv 4, & (23), \\ \text{"} & \text{"} & \equiv 11, & (71), \\ \text{"} & \text{"} & \equiv 37, & (103), \\ \text{"} & \text{"} & \equiv 45, & (151), \\ \text{"} & \text{"} & \equiv 12, & (167). \end{array}$$

Ferner ist

$$\begin{array}{llll} \text{ind } 2 = 2 & \text{mod } 7, \\ \text{ind } 4 = 16 & \text{mod } 23, \\ \text{ind } 11 = 43 & \text{mod } 71, \\ \text{ind } 37 = 81 & \text{mod } 103, \\ \text{ind } 45 = 64 & \text{mod } 151, \\ \text{ind } 12 = 150 & \text{mod } 167. \end{array}$$

Zur Bestätigung der allgemeinen Bemerkung berechnen wir noch

$$\begin{array}{lllll} -1-\sqrt{2} & = -3-\eta^2 & \equiv 3, & (7), \\ \text{"} & \text{"} & \equiv 17, & (23), \\ \text{"} & \text{"} & \equiv 58, & (71), \\ \text{"} & \text{"} & \equiv 64, & (103), \\ \text{"} & \text{"} & \equiv 104, & (151), \\ \text{"} & \text{"} & \equiv 153, & (167). \end{array}$$

Endlich findet man:

$$\begin{array}{ll} \text{ind } 3 \equiv 1, & (7-1), \\ \text{ind } 17 \equiv 17, & (23-1), \\ \text{ind } 58 \equiv 62, & (71-1), \\ \text{ind } 64 \equiv 72, & (103-1), \\ \text{ind } 104 \equiv 11, & (151-1), \\ \text{ind } 153 \equiv 99, & (167-1). \end{array}$$

Somit erhält man

$$\left(\frac{\varepsilon_{1,2}}{\omega_7}\right) = -1, \quad \left(\frac{\varepsilon_{3,4}}{\omega_7}\right) = +1,$$

$$\left(\frac{\varepsilon_{1,2}}{\omega_{23}}\right) = -1, \quad \left(\frac{\varepsilon_{3,4}}{\omega_{23}}\right) = +1,$$

$$\left(\frac{\varepsilon_{1,2}}{\omega_{71}}\right) = +1, \quad \left(\frac{\varepsilon_{3,4}}{\omega_{71}}\right) = -1,$$

$$\left(\frac{\varepsilon_{1,2}}{\omega_{103}}\right) = +1, \quad \left(\frac{\varepsilon_{3,4}}{\omega_{103}}\right) = -1,$$

$$\left(\frac{\varepsilon_{1,2}}{\omega_{151}}\right) = -1, \quad \left(\frac{\varepsilon_{3,4}}{\omega_{151}}\right) = +1,$$

$$\left(\frac{\varepsilon_{1,2}}{\omega_{167}}\right) = -1, \quad \left(\frac{\varepsilon_{3,4}}{\omega_{167}}\right) = +1.$$

6) Unter den Primzahlen ersten Grades sind folgende gewählt:

$$\omega_{17}, \ \omega_{97}, \ \omega_{113}, \ \omega_{193}, \ \omega_{241}, \ \omega_{257}, \ \omega_{353}.$$

Es sind dies Primfaktoren der sämmtlichen rationalen Primzahlen des ersten Tausend von der Form $16m+1$.

Nach (17) findet man in den Tafeln

$$\theta^1 \equiv -7, \quad \theta^3 \equiv -3, \quad \theta^5 \equiv +6, \quad \theta^7 \equiv +5.$$

Darnach berechnet man

$$\left.\begin{aligned} \varepsilon_1 &\equiv 1-\theta+\theta^7 \equiv 13 \\ \varepsilon_2 &\equiv 1+\theta-\theta^7 \equiv \ \ 6 \\ \varepsilon_3 &\equiv 1-\theta^3+\theta^5 \equiv 10 \end{aligned}\right\}, \quad (17),$$

$$\left.\begin{aligned} \text{ind } 13 &\equiv 12 \\ \text{ind } \ 6 &\equiv \ \ 5 \\ \text{ind } 10 &\equiv \ \ 1 \end{aligned}\right\}, \quad (17-1).$$

Hieraus folgt

$$\left(\frac{\varepsilon_1}{\omega_{17}}\right) = +1, \quad \left(\frac{\varepsilon_2}{\omega_{17}}\right) = -1, \quad \left(\frac{\varepsilon_3}{\omega_{17}}\right) = -1.$$

Hierzu fügen wir $\left(\frac{\varepsilon_4}{\omega_{17}}\right) = +1$; denn

$$\left(\frac{\varepsilon_1}{\omega_{17}}\right)\left(\frac{\varepsilon_2}{\omega_{17}}\right)\left(\frac{\varepsilon_3}{\omega_{17}}\right)\left(\frac{\varepsilon^4}{\omega_{17}}\right) = (-1)^{\frac{p-1}{2}} = +1.$$

Auf diese Weise ist das Folgende berechnet worden:

$$\left(\frac{\varepsilon_1}{\omega_{97}}\right) = +1, \quad \left(\frac{\varepsilon_2}{\omega_{97}}\right) = +1, \quad \left(\frac{\varepsilon_3}{\omega_{97}}\right) = -1, \quad \left(\frac{\varepsilon_4}{\omega_{97}}\right) = -1,$$

$$\left(\frac{\varepsilon_1}{\omega_{113}}\right) = +1, \quad \left(\frac{\varepsilon_2}{\omega_{113}}\right) = +1, \quad \left(\frac{\varepsilon_3}{\omega_{113}}\right) = -1, \quad \left(\frac{\varepsilon_4}{\omega_{113}}\right) = -1,$$

$$\left(\frac{\varepsilon_1}{\omega_{193}}\right) = -1, \quad \left(\frac{\varepsilon_2}{\omega_{193}}\right) = +1, \quad \left(\frac{\varepsilon_3}{\omega_{193}}\right) = +1, \quad \left(\frac{\varepsilon_4}{\omega_{193}}\right) = -1,$$

$$\left(\frac{\varepsilon_1}{\omega_{241}}\right) = +1, \quad \left(\frac{\varepsilon_2}{\omega_{211}}\right) = +1, \quad \left(\frac{\varepsilon_3}{\omega_{211}}\right) = +1, \quad \left(\frac{\varepsilon_4}{\omega_{241}}\right) = +1,$$

$$\left(\frac{\varepsilon_1}{\omega_{257}}\right) = +1, \quad \left(\frac{\varepsilon_2}{\omega_{257}}\right) = +1, \quad \left(\frac{\varepsilon_3}{\omega_{257}}\right) = -1, \quad \left(\frac{\varepsilon_4}{\omega_{257}}\right) = -1,$$

$$\left(\frac{\varepsilon_1}{\omega_{353}}\right) = +1, \quad \left(\frac{\varepsilon_2}{\omega_{353}}\right) = +1, \quad \left(\frac{\varepsilon_3}{\omega_{353}}\right) = -1, \quad \left(\frac{\varepsilon_4}{\omega_{353}}\right) = -1.$$

Die Zahl 241 ist von der Form $32m+17$, sodass

$$\left(\frac{\theta}{\omega_{241}}\right) = -1$$

ist. Unter den Primidealen ersten Grades, deren Normen unterhalb 1000 liegen, sind also keine primären anzutreffen.

Aus diesen Berechnungen überzeugen wir uns zuerst, dass ein System von beliebigen drei der Einheiten ε_1, ε_2, ε_3, ε_4 die in § 5 geforderte Eigenschaft besitzt.

Es ergeben sich nämlich aus den Berechnungen folgende drei Zeilen von Gleichungen

$$\text{I.} \quad \left(\frac{\varepsilon_1}{\omega_{\sqrt{-2}}}\right) = \left(\frac{\varepsilon_2}{\omega_{\sqrt{-2}}}\right) = \left(\frac{\varepsilon_3}{\omega_{\sqrt{-2}}}\right) = -1.$$

$$\text{II.} \quad \left(\frac{\varepsilon_1 \cdot \varepsilon_2}{\omega_{73}}\right) = \left(\frac{\varepsilon_1 \cdot \varepsilon_3}{\omega_7}\right) = \left(\frac{\varepsilon_2 \cdot \varepsilon_3}{\omega_7}\right) = -1.$$

$$\text{III.} \quad \left(\frac{\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3}{\omega_{97}}\right) = -1.$$

Aus der ersten Zeile ergiebt sich, dass die Einheiten ε gewiss keine Quadrate sind. Die zweite Zeile sagt aus, dass irgend zwei der Einheiten ε_1, ε_2, ε_3 sich nicht von einer und derselben Grundeinheit durch einen quadratischen Faktor unterscheiden. Die Zeile III endlich bedingt, dass das Produkt aus irgend zwei der Einheiten ε_1, ε_2, ε_3 und die dritte Einheit nicht von einer und derselben Grundeinheit nur um einen quadratischen Faktor unterschieden sind.

Es giebt also unter den Systemen von Grundeinheiten des Körpers $K(\theta)$ gewiss ein solches System von Grundeinheiten η_1, η_2, η_3, dass

$$\begin{aligned} \varepsilon_1 &= \eta_1 \alpha^2 \\ \varepsilon_2 &= \eta_2 \beta^2 \\ \varepsilon_3 &= \eta_3 \gamma^2 \end{aligned}$$

ist, wo α, β, γ irgend welche Einheiten von $K(\theta)$, die 1 nicht ausgeschlossen, bezeichnen.

Da aber die Einheiten $\varepsilon_1, \varepsilon_2, \varepsilon_3$ die durch diese letzten Gleichungen ausgedrückte Eigenschaft besitzen, so sind ihre quadratischen Charaktere identisch mit denjenigen der drei Grundeinheiten η_1, η_2, η_3.

Wir wenden uns jetzt zur Bestätigung des ersten Ergänzungssatzes.

Die Berechnungen ergaben, dass

$$\left(\frac{\theta}{\omega_{\sqrt{-1}}}\right) = \left(\frac{\theta}{\omega_{\sqrt{-2}}}\right) = \left(\frac{\theta}{\omega_{\varrho}}\right) = \left(\frac{\theta}{\omega_{\eta}}\right) = -1$$

und dass

$$\left(\frac{\theta}{\omega_{\theta}}\right) = -1$$

ist, sofern ω_θ ein Primfaktor einer rationalen Primzahl $p = 32m + 17 = 16m + 1$, dass dagegen

$$\left(\frac{\theta}{\omega_{\theta}}\right) = +1$$

ist, falls ω_θ ein Primfaktor einer rationalen Primzahl $p = 32m + 1 = 36m + 1$ ist. Unter diesen letzteren Primzahlen fanden sich, soweit ihre Normen $p < 1000$ ist, keine, nach welchen die drei Einheiten $\varepsilon_1, \varepsilon_2, \varepsilon_3$ sämmtlich als Reste ausfielen.

Die Ideale $(\omega_{\sqrt{-1}})$, $(\omega_{\sqrt{-2}})$, (ω_{ϱ}), (ω_{η}) sowie die in Betracht kommenden Ideale (ω_θ) sind also sämmtlich nicht primär.

Eine besonders ausgezeichnete Stelle nimmt nun der reelle Unterkörper $k(\theta + \theta^{-1}) = k(\vartheta)$ ein, insofern sämmtliche in diesem Körper gelegene Ideale des Körpers $K(\theta)$ primär sind.

In der That werden wir nun zeigen, dass sämmtliche zu 2

prime Zahlen dieses reellen Unterkörpers nach dem Modul 4 stets einer Einheit kongruent sind. Was den Primfaktor von 2 in $k(\vartheta)$, nämlich $2+\vartheta$, betrifft, so ist derselbe ein Quadrat in $K(\theta)$; es ist

$$2+\vartheta = (1+\theta)^2\cdot\left(\frac{1+\theta^{15}}{1+\theta}\right).$$

Wir werden zeigen, dass aus den Einheiten $1-\vartheta$, $1-\vartheta'$, $1-\vartheta''$, $1-\vartheta'''$ ein vollständiges System nach (4) inkongruenter und zu 2 primer Reste des Körpers $k(\vartheta)$ darstellbar ist, woraus folgt, dass jede zu 2 prime Zahl des Körpers $k(\vartheta)$ mit einer geeigneten Einheit dieses Körpers multiplicirt kongruent 1 nach (4) wird.

Der Nachweis hiervon lässt sich auf Grund der im vorigen Paragraphen bereits erkannten Thatsache, dass jede zu 2 prime Zahl des Körpers $k(\sqrt{2})$ irgend einer Einheit dieses Körpers nach (4) kongruent ist, sehr vereinfachen.

Zunächst lässt sich jede Zahl ω_ϑ des Körpers $k(\vartheta)$ in der Form

$$\alpha+\beta\vartheta$$

darstellen, wo α und β Zahlen aus $k(\sqrt{2})$ bezeichnen, von denen α stets dann prim zu 2 ist, wenn ω_ϑ es ist.

Seien also jetzt

$$\text{I.}\quad \alpha_1,\ \alpha_2,\ \alpha_3,\ \ldots\ \alpha_8$$

$\varphi(4)=8$ inkongruente und zu 2 prime Reste in $k(\sqrt{2})$, und

$$\text{II.}\quad \beta_1,\ \beta_2,\ \beta_3,\ \ldots,\ \beta_{16}$$

$n(4)=16$ inkongruente Reste in $k(\sqrt{2})$, so erhält man offenbar ein vollständiges System inkongruenter und zu 2 primer Reste in $k(\vartheta)$, wenn man in dem Ausdruck $\alpha+\beta\vartheta$ jede Zahl α der Reihe I mit jeder Zahl β der Reihe II kombinirt. Von diesen $128=8\cdot16$ Resten $\alpha_i+\beta_k\vartheta$ soll nachgewiesen werden, dass jeder derselben irgend einer Einheit von $k(\vartheta)$ nach (4) kongruent ist.

Nun dürfen wir jede Zahl α der Reihe I einer Einheit η von $k(\sqrt{2})$ nach (4) kongruent setzen. Sei also

$$\alpha\equiv\eta\quad(4),$$

so wird

$$\alpha+\beta\vartheta \equiv \eta+\beta\vartheta, \quad (4).$$

Folglich ist, wenn wir die Einheit $\frac{1}{\eta} = \eta'$ setzen,

$$\alpha+\beta\vartheta \equiv \eta(1+\eta'\beta\vartheta), \quad (4),$$

oder

$$\alpha+\beta\vartheta \equiv \eta(1+\beta'\vartheta) \quad (4),$$

wo β' nach (4) einer der Zahlen der Reihe II kongruent ist.

Wenn also von allen Zahlen $1+\beta\vartheta$, wo β jede Zahl eines vollständigen Restsystemes nach (4) bezeichnet, nachgewiesen ist, dass sie Einheiten von $k(\vartheta)$ nach (4) kongruent sind, so ist dasselbe von allen zu 2 primen Zahlen $\alpha+\beta\vartheta$ überhaupt nachgewiesen.

Die jetzt nur noch in Betracht kommenden 16 Zahlen sind in folgendem Schema enthalten:

$$\begin{array}{ll}
1, & 1+\sqrt{2}\,\vartheta, \\
1+\vartheta, & 1+(1+\sqrt{2})\vartheta, \\
1+2\vartheta, & 1+(2+\sqrt{2})\vartheta, \\
1+3\vartheta, & 1+(3+\sqrt{2})\vartheta, \\
1+2\sqrt{2}\,\vartheta, & 1+3\sqrt{2}\,\vartheta, \\
1+(1+2\sqrt{2})\vartheta, & 1+(1+3\sqrt{2})\vartheta, \\
1+(2+2\sqrt{2})\vartheta, & 1+(2+3\sqrt{2})\vartheta, \\
1+(3+2\sqrt{2})\vartheta, & 1+(3+3\sqrt{2})\vartheta.
\end{array}$$

Der Nachweis, dass diese Zahlen Einheiten von $k(\vartheta)$ nach (4) kongruent sind, lässt sich nun durch eine weitere Ueberlegung auf ein Minimum von Rechnung reduciren.

Gesetzt, dass man gefunden hätte, dass

$$1+(a+b\sqrt{2})\vartheta \equiv (1-\vartheta)^{e_1}(1-\vartheta')^{e_2}(1-\vartheta'')^{e_3}(1-\vartheta''')^{e_4},$$

nach (4) sei, wo a, b, sowie e_1, e_2, e_3, e_4 ganze rationale Zahlen bezeichnen, so wird auch für alle diejenigen Zahlen, welche aus $1+(a+b\sqrt{2})\vartheta$ durch eine cyklische Substitution des Körpers $k(\vartheta)$ hervorgegangen sind, nachgewiesen sein, dass sie Einheiten von $k(\vartheta)$ nach (4) kongruent sind, denjenigen Einheiten nämlich, welche

aus der rechten Seite obiger Kongruenz durch Anwendung derselben cyklischen Substitution auf ϑ, ϑ', ϑ'', ϑ''' hervorgehen.

In § 1 (Seite 3) sind die cyklischen Substitutionen der Substitutionsgruppe des reellen Unterkörpers von $K(Z)$ allgemein angegeben; es sind dies in unserem Falle die Potenzen der Substitution $s = (\theta : \theta^5)$ von der ersten Potenz bis zur vierten.

Wir greifen die beiden Substionen

$$s^2 = (\theta : -\theta) \quad \text{und} \quad s^3 = (\theta : -\theta^5)$$

heraus. Da nun $\vartheta = \theta - \theta^7$, $\vartheta'' = \theta^3 - \theta^5$ gesetzt ist und da $\vartheta' = -\vartheta$, $\vartheta''' = -\vartheta''$, $\sqrt{2} = \theta^2 - \theta^6$ ist, so wird durch die Substitution s^2

$$\begin{array}{lcl} -\vartheta \text{ oder } \vartheta' & \text{aus} & \vartheta \\ +\sqrt{2} & \text{„} & +\sqrt{2} \\ -\vartheta'' \text{ oder } \vartheta''' & \text{„} & \vartheta'', \end{array}$$

und durch die Substitution s^3

$$\begin{array}{lcl} \vartheta'' & \text{aus} & \vartheta \\ -\sqrt{2} & \text{„} & +\sqrt{2} \\ -\vartheta & \text{„} & \vartheta''. \end{array}$$

Wir werden jetzt zeigen, dass die einzigen Zahlen des obigen Schemas, von denen nachzuweisen ist, dass sie Einheiten nach (4) kongruent sind, nur die 4 folgenden sind:

$$\begin{array}{ll} 1 + \sqrt{2}\,\vartheta, & 1 + 2\vartheta, \\ 1 + 2\sqrt{2}\,\vartheta, & 1 + (1 + \sqrt{2})\vartheta. \end{array}$$

Man findet nach dem Modul 4:

$$(1.) \quad 1 + \sqrt{2}\,\vartheta \equiv (1 + \vartheta)^2 (1 + \vartheta'').$$

Daraus folgert man, indem man auf beiden Seiten die cyklische Substitution

$$s^2 = (\theta : -\theta) = \begin{pmatrix} \vartheta : -\vartheta \\ \vartheta'' : -\vartheta'' \\ +\sqrt{2} : +\sqrt{2} \end{pmatrix}$$

anwendet,

$$1 + 3\sqrt{2} \equiv (1 - \vartheta)^2 (1 - \vartheta''),$$

und hieraus durch Anwendung der Substitution

$$s^2 = (\theta : -\theta^5) = \begin{pmatrix} \vartheta'' : \vartheta \\ -\vartheta : \vartheta'' \\ -\sqrt{2} : +\sqrt{2} \end{pmatrix}$$

die Kongruenz:

$$1 + (2 + 3\sqrt{2})\vartheta \equiv (1 - \vartheta'')^3 (1 + \vartheta);$$

wendet man auf diese Kongruenz s^2 an, so kommt noch

$$1 + (2 + \sqrt{2})\vartheta \equiv (1 + \vartheta'')^3 (1 - \vartheta).$$

Zweitens findet man

$$(2.) \quad 1 + (1 + \sqrt{2})\vartheta \equiv -(1 \pm \vartheta)^2 (1 - \vartheta'')^2,$$

wo $(1 \pm \vartheta)^2$ geschrieben ist, wegen

$$(1 + \vartheta)^2 \equiv (1 - \vartheta)^2.$$

Aus (2) erhält man vermöge der Substitution s^2

$$1 + (3 + 3\sqrt{2})\vartheta \equiv -(1 \pm \vartheta)^2 (1 + \vartheta'')^2.$$

Hieraus folgt durch Anwendung der Substitution s^3:

$$1 + (3 + 2\sqrt{2}) \equiv -(1 \pm \vartheta'')^2 (1 - \vartheta)^2,$$

woraus man vermöge Anwendung von s^2

$$1 + (1 + 2\sqrt{2})\vartheta \equiv -(1 \pm \vartheta'')^2 (1 + \vartheta)^2,$$

erhält.

Drittens ist

$$(3.) \quad 1 + 2\sqrt{2}\,\vartheta \equiv -(1 \pm \vartheta)^2 (1 \pm \vartheta'')^2,$$

woraus durch Anwendung cyklischer Substitutionen keine weiteren Zahlen erhalten werden, was erstens seinen Grund darin hat, dass

$$(1 + \vartheta)^2 \equiv (1 - \vartheta)^2$$
$$(1 + \vartheta'')^2 \equiv (1 - \vartheta'')^2,$$

und sodann darin, dass die rechte Seite der Kongruenz

$$(1 \pm \vartheta)^2 (1 \pm \vartheta'')^2$$

symmetrisch in Bezug auf ϑ, ϑ'' ist, sodass durch Vertauschung dieser Zahlen der Ausdruck ungeändert bleibt.

An vierter Stelle hat man noch

$$(4.)\quad 1+2\vartheta \equiv (1-\sqrt{2})(1\pm\vartheta'')^2,$$

woraus durch Anwendung der Substitution s^2 folgt:

$$1+(2+2\sqrt{2})\vartheta \equiv (1+\sqrt{2})(1\pm\vartheta)^2.$$

Wir haben bis jetzt 11 Zahlen des obigen Schemas durch nach (4) kongruente Einheiten dargestellt; hierzu kommen noch folgende Kongruenzen

$$\begin{aligned} 1+\vartheta &\equiv 1+\vartheta \\ 1+3\vartheta &\equiv 1-\vartheta \\ 1+(3+\sqrt{2})\vartheta &\equiv 1+\vartheta'' \\ 1+(1+3\sqrt{2})\vartheta &\equiv 1+\vartheta'' \\ 1 &\equiv 1, \end{aligned}$$

womit alle Zahlen des obigen Schemas durch kongruente Einheiten dargestellt und unsere Behauptung bewiesen ist.

Wir sprechen das Resultat der Bestätigung des ersten Ergänzungssatzes in folgendem Satze aus:

Satz 7. Diejenigen Primideale des Körpers $K(\theta)$, welche in dem reellen Unterkörper $k(\theta+\theta^{-1})$ liegen, sind sämmtlich primär; ist $\mathfrak{o}$ ein solches primäres Primideal, so giebt es stets eine primäre Zahl ω, sodass $\mathfrak{o} = (\omega)$ und

$$\omega \equiv 1, \quad (4)$$

ist.

Wir wenden uns zur Bestimmung der hyperprimären Primideale und zur Bestätigung des zweiten Ergänzungssatzes.

Gemäss der Definition 3 des § 6 wird ein primäres Ideal des Körpers $K(\theta)$, also in unserem Falle ein Hauptideal (ω_ϑ), dann hyperprimär heissen, wenn

$$\left(\frac{1+\theta}{\omega_\vartheta}\right) = +1$$

ausfällt, wo $1+\theta$ Primfaktor der Zahl 2 ist. Es ist $2 = \varepsilon\cdot(1+\theta)^8$, wo ε eine Einheit bezeichnet.

Man hat also als Ansatz folgende Kongruenz nach (ω_ϑ):

$$\left(\frac{1+\theta}{\omega_\vartheta}\right) \equiv (1+\theta)^{\frac{n(\omega_\vartheta)-1}{2}};$$

hier ist die Norm $n(\omega_\vartheta) = p^2$ und p von der Form $16m+15$.

Es ist also

$$\left(\frac{1+\theta}{\omega_\vartheta}\right) \equiv (1+\theta)^{\frac{p^2-1}{2}}$$
$$\equiv \{(1+\theta)(1+\theta^{15})\}^{\frac{p-1}{2}}$$
$$\equiv (2+\vartheta)^{\frac{p-1}{2}}.$$

Nun bemerke man erstens, dass $\sqrt{2+\vartheta}$ die bestimmende Zahl des reellen Unterkörpers des Zahlkörpers $K(\sqrt{\theta}) = K\left(e^{\frac{2i\pi}{2^6}}\right)$, und dass ferner, gemäss dem Schluss des § 3, die rationalen Primzahlen $p = 32m+31$, welche in der Form $p = 16m+15$ mit inbegriffen sind, im Körper $k(\sqrt{2+\vartheta})$ in Primideale des Körpers $K(\sqrt{\theta})$ zerlegt werden, sodass nach dem ersten Teile des Satzes 1 in § 3

$$\sqrt{2+\vartheta}^{\,p} = \sqrt{2+\vartheta}$$

wird, während, wenn p von der Form $32m+15$ ist, die Substitution $\sigma = \left(\sqrt{2+\vartheta} : \sqrt{2+\vartheta}^{\,p}\right)$ eine Relativsubstitution des Körpers $k(\sqrt{2+\vartheta})$ in Bezng den Unterkörper $k(\vartheta)$ ist, sodass hier

$$\sqrt{2+\vartheta}^{\,p} = -\sqrt{2+\vartheta}$$

wird.

Hieraus folgt, dass

$$\left(\frac{1+\theta}{\omega_\vartheta}\right) \equiv \sqrt{2+\vartheta}^{\,p-1} = +1,$$

für $p = 32m+31$, und

$$\left(\frac{1+\theta}{\omega_\vartheta}\right) \equiv \sqrt{2+\vartheta}^{\,p-1} = -1,$$

für $p = 32m+15$.

Wir zeigen jetzt, in Bestätigung des zweiten Ergänzungssatzes, von allen denjenigen Primzahlen ω_ϑ des Körpers $K(\theta)$, welche Primfaktoren der rationalen Primzahlen $p = 32m+31$ sind, wo $p < 1000$, dass dieselben einer Einheit des Körpers $k(\vartheta)$ nach dem Modul (4ϑ), also erst recht nach dem Modul $4(1+\theta)$, wo $\varepsilon \cdot (1+\theta)^2 = \vartheta$, kongruent sind, dass dieselben also mit einer geeigneten Einheit von $k(\vartheta)$ multiplicirt kongruent 1 nach (4ϑ) sind.

Die auf der linken Seite der folgenden Kongruenzen stehenden Primzahlen sind den Tabellen von Reuschle entnommen.

$$\begin{aligned}
\omega_{31} &= 3+2\vartheta \equiv \left(-1+\sqrt{2}\right)(1 \pm \vartheta'')^2, \\
\omega_{127} &= 1-3\vartheta'' \equiv 1+\vartheta'', \\
\omega_{223} &= 7+4\vartheta \equiv -1, \\
\omega_{383} &= 5+6\vartheta \equiv \left(1-\sqrt{2}\right)(1 \pm \vartheta'')^2, \\
\omega_{479} &= 7+3\vartheta+3\vartheta'' \equiv -(1+\vartheta'')(1+\vartheta)^2, \\
\omega_{607} &= 3+4\vartheta+2\vartheta'' \equiv \left(-1+\sqrt{2}\right)(1+\vartheta)^2, \\
\omega_{863} &= 15-4\vartheta-9\vartheta'' \equiv -(1+\vartheta'') \\
\omega_{991} &= 1-4\vartheta+\vartheta'' \equiv 1+\vartheta'',
\end{aligned}$$

wo der Modul 4ϑ, bezw. $4\vartheta''$ ist.

Das Korollar des Satzes 3 des § 6:

„Sind ν, μ ganze zu 2 prime Zahlen des Körpers k und ist mindestens eine der Zahlen ν, μ primär, so ist

$$\left(\frac{\nu}{\mu}\right) = \left(\frac{\mu}{\nu}\right)\text{“},$$

werden wir für eine unendliche Anzahl von Primzahlen des Körpers $K(\theta)$ bestätigen.

Auf Grund der Sätze des § 4 und indem wir infolge des Satzes 7 die Primärzahl $\omega_\vartheta \equiv 1, (4)$ voraussetzen, führen wir die Richtigkeit der Gleichungen:

$$\text{I.} \quad \left(\frac{\omega_\vartheta}{\omega_\eta}\right) = \left(\frac{\omega_\eta}{\omega_\vartheta}\right).$$

$$\text{II.} \quad \left(\frac{\omega_\vartheta}{\omega_\varrho}\right) = \left(\frac{\omega_\varrho}{\omega_\vartheta}\right).$$

$$\text{III.} \quad \left(\frac{\omega_\vartheta}{\omega_{\sqrt{-1}}}\right) = \left(\frac{\omega_{\sqrt{-1}}}{\omega_\vartheta}\right).$$

$$\text{IV.}\quad \left(\frac{\omega_{\vartheta}}{\omega_{\sqrt{-2}}}\right) = \left(\frac{\omega_{\sqrt{-2}}}{\omega_{\vartheta}}\right)$$

auf die Giltigkeit des Reciprocitätsgesetzes im Körper $k(\varrho)$ und im Körper der rationalen Zahlen zurück.

Mögen die Primzahlen $\omega_{\vartheta}, \omega_{\eta}, \omega_{\varrho}, \omega_{\sqrt{-1}}, \omega_{\sqrt{-2}}$ bezw. Teiler der rationalen Primzahlen p, q_1, q_2, q_3, q_4 sein, so hat man zuerst folgenden Ansatz

$$\left(\frac{\omega_{\vartheta}}{\omega_{\eta}}\right) \equiv \left\{N_{k(\eta)}(\omega_{\vartheta})\right\}^{\frac{q_1-1}{2}}, \quad (\omega_{\eta})$$

$$\left(\frac{\omega_{\eta}}{\omega_{\vartheta}}\right) \equiv \left\{N_{k(\vartheta)}(\omega_{\eta})\right\}^{\frac{p-1}{2}}, \quad (\omega_{\vartheta}).$$

Nach Satz 5 § 4 müssen die Relativnormen auf der rechten Seite der Kongruenzen Primzahlen ersten Grades des den Körpern $k(\vartheta)$ und $k(\eta)$ gemeinsamen Unterkörpers $k(\sqrt{2})$ sein; wir bezeichnen $N_{k(\eta)}(\omega_{\vartheta})$ mit $\omega_{\sqrt{2}}$ und $N_{k(\vartheta)}(\omega_{\eta})$ mit $\omega'_{\sqrt{2}}$ und werden zeigen, dass

$$\omega_{\sqrt{2}}^{\frac{q_1-1}{2}} = \omega'^{\frac{p-1}{2}}_{\sqrt{2}}$$

also

$$\left(\frac{\omega_{\vartheta}}{\omega_{\eta}}\right) = \left(\frac{\omega_{\eta}}{\omega_{\vartheta}}\right)$$

ist.

Ferner ist

$$\left(\frac{\omega_{\vartheta}}{\omega_{\varrho}}\right) \equiv \left\{N_{k(\varrho)}(\omega_{\vartheta})\right\}^{\frac{q_2-1}{2}}, \quad (\omega_{\varrho}),$$

$$\left(\frac{\omega_{\varrho}}{\omega_{\vartheta}}\right) \equiv \left\{N_{k(\vartheta)}(\omega_{\varrho})\right\}^{\frac{p-1}{2}}, \quad (\omega_{\vartheta}).$$

Setzen wir gemäss Satz 5 § 4

$$N_{k(\varrho)}(\omega_{\vartheta}) = \omega_{\sqrt{2}}$$

$$N_{k(\vartheta)}(\omega_{\varrho}) = \omega''_{\sqrt{2}},$$

so folgt die Richtigkeit der Gleichung

$$\left(\frac{\omega_{\vartheta}}{\omega_{\varrho}}\right) = \left(\frac{\omega_{\varrho}}{\omega_{\vartheta}}\right)$$

aus der sogleich zu beweisenden Gleichung

$$\omega_{\sqrt{2}}^{\frac{q_2-1}{2}} = \omega''^{\frac{p-1}{2}}_{\sqrt{2}}.$$

In der That ist erstens

$$\omega_{\sqrt{2}}^{\frac{q_2-1}{2}} = \omega''^{\frac{p-1}{2}}_{\sqrt{2}}$$

oder

$$\left(\frac{\omega_{\sqrt{2}}}{\omega'_{\sqrt{2}}}\right) = \left(\frac{\omega'_{\sqrt{2}}}{\omega_{\sqrt{2}}}\right)$$

in $k(\sqrt{2})$, da $\omega_\vartheta \equiv 1,\ (4)$, also auch die Relativnorm $\omega_{\sqrt{2}} \equiv 1,\ (4)$ ist.

Zweitens ist

$$\omega_{\sqrt{2}}^{\frac{q_2-1}{2}} = \omega_{\sqrt{2}}^{\frac{p-1}{2}}$$

oder

$$\left(\frac{\omega_{\sqrt{2}}}{\omega''_{\sqrt{2}}}\right) = \left(\frac{\omega''_{\sqrt{2}}}{\omega_{\sqrt{2}}}\right)$$

in $k(\sqrt{2})$, aus ebendemselben Grunde.

Wie wir nun die Richtigkeit der Gleichungen I und II auf die Richtigkeit des Reciprocitätsgesetzes in $k(\sqrt{2})$ zurückgeführt haben, so führen wir nunmehr die Richtigkeit der Gleichungen III und IV auf das Reciprocitätsgesetz im Körper der rationalen Zahlen zurück.

Man hat zuerst den Ansatz

$$\left(\frac{\omega_\vartheta}{\omega_{\sqrt{-1}}}\right) \equiv \left\{N_{k(\sqrt{-1})}(\omega_\vartheta)\right\}^{\frac{q_2-1}{2}}, \quad (\omega_{\sqrt{-1}}),$$

$$\left(\frac{\omega_{\sqrt{-1}}}{\omega_\vartheta}\right) \equiv \left\{N_{k(\vartheta)}(\omega_{\sqrt{-1}})\right\}^{\frac{p-1}{2}}, \quad (\omega_\vartheta).$$

Nach Satz 5 § 4 liegen die Relativnormen rechter Hand der Kongruenzen im Körper der rationalen Zahlen, und sind dort Primzahlen ersten Grades. Da ferner nach Voraussetzung $\omega_\vartheta \equiv 1$, (4), so ist auch

$$N_{k(\sqrt{-1})}(\omega_\vartheta) \equiv 1, \quad (4),$$

also

$$N_{k(\sqrt{-1})}(\omega_\vartheta) = -p,$$

weil p von der Form $16m+15$ ist.

Jetzt folgt die Richtigkeit der Gleichung

$$\left(\frac{\omega_\vartheta}{\omega_{\sqrt{-1}}}\right) = \left(\frac{\omega_{\sqrt{-1}}}{\omega_\vartheta}\right)$$

aus der Richtigkeit der Gleichung

$$(-p)^{\frac{q_3-1}{2}} \equiv (\pm q_3)^{\frac{p-1}{2}}$$

oder aus

$$\left(\frac{-p}{q_3}\right) = \left(\frac{\pm q_3}{p}\right).$$

Die Richtigkeit der Gleichung IV

$$\left(\frac{\omega_\vartheta}{\omega_{\sqrt{-2}}}\right) = \left(\frac{\omega_{\sqrt{-2}}}{\omega_\vartheta}\right)$$

folgt aus der Gleichung

$$(-p)^{\frac{q_4-1}{2}} = (\pm q_4)^{\frac{p-1}{2}}$$

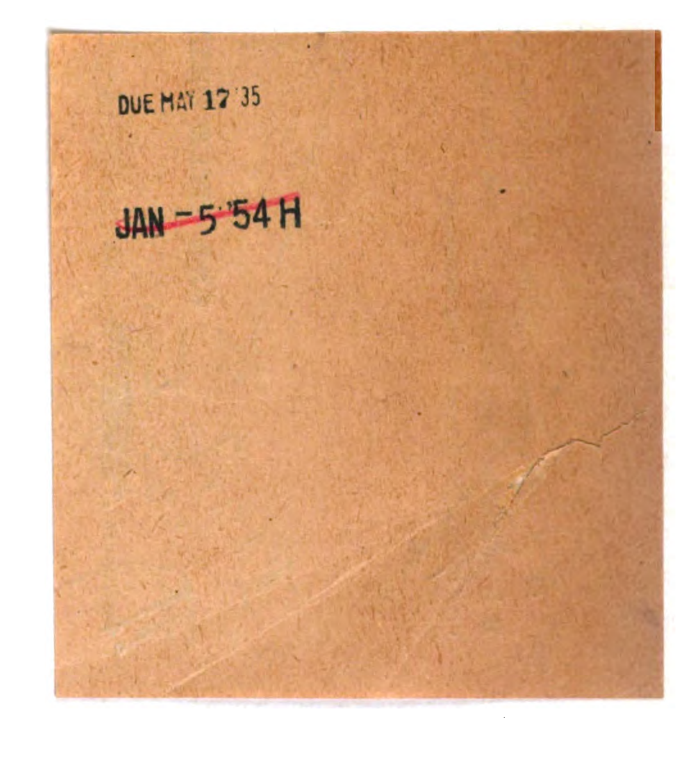
oder aus

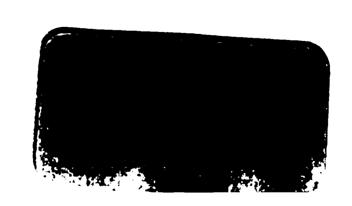
$$\left(\frac{-p}{q_4}\right) = \left(\frac{\pm q_4}{p}\right).$$

Vita.

Ich bin am 27ten Februar 1868 zu Langenbielau in Schlesien geboren. Ich besuchte das humanistische Gymnasium zu Schweidnitz, wo meine Neigung geteilt war zwischen dem klassischen Altertum und dem rein Abstrakten und Philosophischen. Als einem Gegengewicht meiner Neigung zu dem rein Abstrakten widmete ich mich im Beginn der akademischen Studienzeit den Erfahrungswissenschaften der Chemie und Physik, pflegte aber noch weiterhin das schon frühe begonnene Studium der spekulativen Philosophie von Kant und Schopenhauer und des philosophischen Teiles der Werke von Goethe und besonders von Schiller. Ich hörte bei den Herren Professoren Viktor Meyer, A. W. v. Hofmann, Kundt, Benno Erdmann, Kuno Fischer, Wundt.

Erst in vorgerückten Semestern hörte ich zum ersten Male über Mathematik und entschied mich für diese Wissenschaft, als meinem Hauptfache. In die Analysis wurde ich im siebenten Semester durch Leo Königsberger eingeführt. In Leipzig studierte ich die Grundzüge der Lie'schen Geometrie und widmete mich ebendaselbst dem Studium älterer klassischer Abhandlungen, insbesondere von Euler und Lagrange. Meine letzten Studien in Göttingen betreffen Zahlentheorie, Mechanik, Funktionentheorie und mechanische Theorie der Wärme. Zu besonderem Danke bin ich in Göttingen dem eindringlichen Vortrage der Herren Professoren David Hilbert und Felix Klein verpflichtet.


DUE MAY 17 '35
JAN - 5 '54 H




Math 1609.00.3
Das allgemeine quadratische recipro
Cabot Science 003307973
3 2044 091 895 789
Digitized by Google